The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION **APRIL 2022**

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 **NUMBER 4** **April 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

Federal Trade Commission Expands Data Security Safeguards Requirements

By Michael J. Heller*

In this article, the author discusses a newly updated rule announced recently by the Federal Trade Commission that increases the data security safeguards that financial institutions must put in place to protect their customers' confidential information.

In recent years, widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft and other forms of financial distress. State and federal regulators of course have taken notice and as a consequence have imposed a variety of requirements on financial institutions intended to protect consumers' confidential information.[1]

Now, the Federal Trade Commission (the "FTC" or the "Commission") has issued a final rule (the "Final Rule") amending its Standards for Safeguarding Customer Information (the "Safeguards Rule" or the "Rule") with respect to the handling of customer information by financial institutions over which the FTC has jurisdiction.

The amended Safeguards Rule contains five main modifications to the existing Rule.

First, the amended Safeguards Rule adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication and encryption.

Second, the amended Safeguards Rule adds provisions intended by the FTC to improve the accountability of financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies.

Third, the amended Safeguards Rule exempts financial institutions that maintain customer information concerning fewer than 5,000 consumers from certain requirements of the amended Rule.

---

* Michael J. Heller, a member of the Banking, Corporate, and Real Estate Practice Groups at Rivkin Radler LLP and a member of the Board of Editors of *The Banking Law Journal*, works extensively with bank clients on complex commercial loans, including Industrial Development Agency and Small Business Administration matters, and with private clients in real estate development and corporate transactions. He may be reached at michael.heller@rivkin.com.

[1] *See, e.g.,* Michael J. Heller, "Banks May Face New Computer-Security Incident Notification Requirements," *Banking L. J.* (June 2021).

Fourth, the amended Safeguards Rule expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. This change adds "finders"—companies that bring together buyers and sellers of a product or service—within the scope of the amended Rule.

Finally, the amended Safeguards Rule defines several terms in the Rule itself rather than have them incorporated by reference from the FTC's Privacy of Consumer Financial Information Rule (the "Privacy Rule").[2]

This article discusses the significant changes to the Safeguards Rule and the implications for financial institutions.

BACKGROUND

Congress enacted the Gramm-Leach-Bliley Act (the "GLB") in 1999.[3] The GLB provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, the GLB 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 GLB required the Commission and other federal agencies to establish standards for financial institutions relating to administrative, technical and physical safeguards for certain information.[4] Pursuant to the GLB's directive, the Commission promulgated the Safeguards Rule in 2002; it became effective on May 23, 2003.

Since then, the Safeguards Rule has required a financial institution to develop, implement and maintain a comprehensive information security program that consists of the administrative, technical and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.[5] Under the Safeguards Rule, the information security program must be written in one or more readily accessible parts.[6]

Moreover, the safeguards set forth in the program must be appropriate to the size and complexity of the financial institution, the nature and scope of its

---

[2] 16 CFR part 313.

[3] Pub. L. 106-102, 113 Stat. 1338 (1999).

[4] *See* 15 U.S.C. 6801(b), 6805(b)(2).

[5] 16 CFR 314.2(c).

[6] 16 CFR 314.3(a).

activities, and the sensitivity of any customer information at issue.[7] The safeguards also must be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[8]

To develop, implement and maintain an information security program, a financial institution must identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information.[9] The financial institution then must design and implement safeguards to control the risks identified through the risk assessment, and must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures.[10] The Safeguards Rule also requires the financial institution to evaluate and adjust its information security program in light of the results of this testing and monitoring, any material changes in its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.[11] The financial institution also must designate an employee or employees to coordinate the information security program.[12]

Finally, financial institutions have been required to take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information and to require those service providers by contract to implement and maintain such safeguards.[13]

REGULATORY REVIEW

On September 7, 2016, the Commission solicited comments on the Safeguards Rule as part of its periodic review of its rules and guides.[14] On April 4, 2019, after receiving more than two dozen comments from individuals and

---

[7] 16 CFR 314.3(a), (b).

[8] 16 CFR 314.3(a), (b).

[9] 16 CFR 314.4(b).

[10] 16 CFR 314.4(c).

[11] 16 CFR 314.4(e).

[12] 16 CFR 314.4(a).

[13] 16 CFR 314.4(d).

[14] Safeguards Rule, Request for Comment, 81 FR 61632 (Sept. 7, 2016).

entities, the Commission issued a Notice of Proposed Rulemaking ("NPRM") setting forth proposed amendments to the Safeguards Rule (the "Proposed Rule").[15]

In response, the Commission received dozens of additional comments from various interested parties. It now has issued final amendments to the Safeguards Rule.

OVERVIEW OF FINAL RULE

As noted above, the Final Rule modifies the former Rule in five primary ways.

First, the Final Rule amends the former Rule to include more detailed requirements for the development and establishment of the information security program required under the Rule. For example, while the former Rule requires financial institutions to undertake a risk assessment and develop and implement safeguards to address the identified risks, the Final Rule sets forth specific criteria for what the risk assessment must include, and requires that the risk assessment be set forth in writing. As to particular safeguards, the Final Rule requires that they address access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, testing and incident response. And while the Final Rule retains the requirement from the former Rule that financial institutions provide employee training and appropriate oversight of service providers, it adds mechanisms designed, according to the FTC, to ensure that such training and oversight are effective. Although the Final Rule has more specific requirements than the former Rule, in the FTC's opinion it still provides financial institutions the flexibility to design an information security program that is appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.

Second, the Final Rule adds requirements designed to improve accountability of financial institutions' information security programs. For example, while the former Rule allows a financial institution to designate one or more employees to be responsible for the information security program, the Final Rule requires the designation of a single "Qualified Individual." The Final Rule also requires periodic reports to boards of directors or governing bodies, which the FTC believes will provide senior management with better awareness of their financial

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

institutions' information security programs, making it more likely that the programs will receive the required resources and be able to protect consumer information.

Third, the FTC recognized the impact of the additional requirements on small businesses and the Final Rule exempts financial institutions that collect information on fewer than 5,000 consumers from the requirements of a written risk assessment, incident response plan and annual reporting to the board of directors.

Fourth, the Final Rule expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. This change brings "finders"—companies that bring together buyers and sellers of a product or service—within the scope of the Rule. Finders often collect and maintain very sensitive consumer financial information, and this change will require them to comply with the Safeguards Rule's requirements to protect that information. This change also will bring the Rule into harmony with other federal agencies' Safeguards Rules, which include activities incidental to financial activities in their definition of financial institution.

Finally, the Final Rule includes several definitions and related examples, including of "financial institution," in the Rule itself rather than incorporate them by reference from a related FTC rule, the Privacy Rule. The FTC said that it believes that this will make the Rule more self-contained and more understandable without a need to reference the Privacy Rule.

KEY DEFINITIONS

The Final Rule contains a number of important definitions.

For example, the Final Rule defines "security event" as "an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form." The term "customer information" means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.

As another example, the Final Rule defines "encryption" as "the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material." This definition does not require any specific process or

technology to perform the encryption but does require that whatever process is used be sufficiently robust to prevent the deciphering of the information in most circumstances.

In addition, the Final Rule now defines "information system" as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or any such system connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems, that contains customer information or that is connected to a system that contains customer information."

Significantly, the Final Rule made one substantive change to the definition of "financial institution" that it incorporated from the Privacy Rule. In addition to mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission, the term now also includes entities that act as "finders." Specifically, the term includes entities that are "significantly engaged in activities that are incidental to [] financial activity" as defined by the Bank Holding Company Act. This change brings the act of "finding" as defined in 12 CFR 225.86(d)(1) into the definition of financial institution.

This change to the definition of "financial institution" brings it into harmony with other agencies' GLB rules.[16] The GLB defines a "financial institution" as any institution "the business of which is engaging in financial activities as described in section 1843(k) of title 12."[17] That section, in turn, describes activities that are financial in nature as those that the Federal Reserve Board has determined "to be financial in nature or incidental to such financial activity."[18]

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

As provided in the Final Rule, financial institutions must develop, implement and maintain a comprehensive information security program that is written in

---

[16] *See* 12 CFR 1016.3(l) (defining "financial institution" for entities regulated by agencies other than the FTC). *See also* 17 CFR 248.3(n) (defining "financial institution" to include "any institution the business of which is . . . incidental to . . . financial activities" for Security and Exchange Commission's rule implementing GLB's safeguard provisions).

[17] 15 U.S.C. 6809(3).

[18] 12 U.S.C. 1843(k).

one or more readily accessible parts and contains administrative, technical and physical safeguards that are appropriate to their size and complexity, the nature and scope of their activities and the sensitivity of any customer information at issue. The information security program must include the elements set forth below.

In order to develop, implement, and maintain an information security program, a financial institution subject to the Final Rule must:

- Designate a qualified individual responsible for overseeing and implementing its information security program and enforcing its information security program ("Qualified Individual"). The Qualified Individual may be employed by the financial institution, an affiliate, or a service provider. To the extent this requirement is met using a service provider or an affiliate, the financial institution must:
    - Retain responsibility for compliance with this part;
    - Designate a senior member of its personnel responsible for direction and oversight of the Qualified Individual; and
    - Require the service provider or affiliate to maintain an information security program that protects the financial institution.
- Base its information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and that assesses the sufficiency of any safeguards in place to control these risks.
- The risk assessment must be written and include:
    - Criteria for the evaluation and categorization of identified security risks or threats the financial institution faces;
    - Criteria for the assessment of the confidentiality, integrity and availability of the financial institution's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats it faces; and
    - Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.
- Periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security,

confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and that reassess the sufficiency of any safeguards in place to control these risks.

- Design and implement safeguards to control the risks the financial institution identifies through risk assessment, including by:
    - Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to (1) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information, and (2) limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;
    - Identifying and managing the data, personnel, devices, systems and facilities that enable the financial institution to achieve business purposes in accordance with their relative importance to business objectives and the financial institution's risk strategy;
    - Protecting by encryption all customer information held or transmitted by the financial institution both in transit over external networks and at rest. To the extent the financial institution determines that encryption of customer information, either in transit over external networks or at rest, is infeasible, the financial institution may instead secure such customer information using effective alternative compensating controls reviewed and approved by the financial institution's Qualified Individual;
    - Adopting secure development practices for in-house developed applications used by the financial institution for transmitting, accessing, or storing customer information and procedures for evaluating, assessing or testing the security of externally developed applications the financial institution uses to transmit, access or store customer information;
    - Implementing multi-factor authentication for any individual accessing any information system, unless the financial institution's Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;
    - Developing, implementing and maintaining procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in

connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained, and periodically review the financial institution's data retention policy to minimize the unnecessary retention of data;

- Adopting procedures for change management; and
- Implementing policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments.
- Implement policies and procedures to ensure that personnel are able to enact the information security program by:
  - Providing the financial institution's personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
  - Using qualified information security personnel employed by the financial institution or an affiliate or service provider sufficient to manage the information security risks and to perform or oversee the information security program;
  - Providing information security personnel with security updates and training sufficient to address relevant security risks; and
  - Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.
- Oversee service providers by:
  - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

  - Requiring the financial institution's service providers by contract to implement and maintain such safeguards; and
  - Periodically assessing the financial institution's service providers based on the risk they present and the continued adequacy of their safeguards.
- Evaluate and adjust the information security program in light of the results of the testing and monitoring required above; any material changes to operations or business arrangements; the results of risk assessments; or any other circumstances that the financial institution knows or has reason to know may have a material impact on its information security program.
- Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity or availability of customer information in the financial institution's control.

CONCLUSION

The Final Rule provides that certain elements of the information security program are not required until one year after the publication of the Final Rule, that is, December 2022. The provisions with a one-year delayed effective date include those that relate to the appointment of a "Qualified Individual," conducting a written risk assessment, the new elements of the information security program, training for personnel, periodic assessment of service providers, preparation of a written incident response plan, and preparation of annual written reports from the Qualified Individual.

In addition, financial institutions that maintain customer information concerning fewer than 5,000 consumers are exempted from the requirements relating to a written risk assessment, continuous monitoring or annual penetration testing and biannual vulnerability assessment, a written incident response plan, and an annual written report by the Qualified Individual.

Importantly, the addition of more detailed requirements under the Final Rule may require some financial institutions to perform additional risk assessments or monitoring, or to create additional safeguards as set forth in the Final Rule. These obligations may require institutions to retain employees or third-party service providers with skills in information security. There also may be additional related compliance costs (e.g., legal, new equipment or systems, modifications to policies or procedures).

If they have not already done so, financial institutions subject to the Final Rule should begin to consider how they will be complying with the new

requirements and budgeting for the increased costs that they are likely to incur. The deadline for complying with the Final Rule is fast approaching.