The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION FEBRUARY 2022

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 **NUMBER 2** **February 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.

FTC Releases Detailed Information Security Requirements and Proposes Breach Notification for Financial Institutions

Duane C. Pozza, Antonio J. Reynolds and Stephen J. Conley*

The authors of this article explain the Federal Trade Commission's announced revisions to its Safeguards Rule, which requires certain financial institutions to implement information security programs to protect consumer financial information.

The Federal Trade Commission ("FTC") announced revisions[1] to its Safeguards Rule[2] ("Revised Safeguards Rule"), which requires certain financial institutions to implement information security programs to protect consumer financial information. The FTC's Safeguards Rule covers a range of companies that engage in financial activities and are subject to the Gramm-Leach-Bliley Act ("GLBA"), including many online financial technology ("Fintech") companies, mortgage lenders, and companies otherwise involved in credit transactions, among others.

The FTC voted 3-2 along party lines to approve the Revised Safeguards Rule, with Commissioners Khan and Slaughter issuing a joint statement[3] and Commissioners Phillips and Wilson releasing a dissenting statement.[4] While the joint statement praised the Revised Safeguards Rule as an effort to "meet the challenges of today's security environment," the dissenting statement criticized the regulations as a "one-size-fits-all" approach to data security that may not be flexible enough to meet its goals.

---

* Duane C. Pozza is a partner at Wiley Rein LLP advising clients on complex legal and regulatory issues involving emerging technology, consumer protection, and Federal Trade Commission enforcement. Antonio J. Reynolds is a partner at the firm representing financial services companies and other major corporations, as well as their officers and directors, in a variety of civil and criminal enforcement matters before federal and state agencies. Stephen J. Conley is an associate at the firm providing regulatory counsel on a wide array of issues related to privacy, telecommunications, and technology. The authors may be reached at dpozza@wiley.law, areynolds@wiley.law and sconley@wiley.law, respectively.

1 https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial?utm_source=govdelivery.

2 https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-314-standards-safeguarding-customer-information-final. The Revised Rule was published in the Federal Register on December 9, 2021.

3 https://www.ftc.gov/public-statements/2021/10/statement-chair-lina-m-khan-joined-commissioner-rebecca-kelly-slaughter.

4 https://www.ftc.gov/public-statements/2021/10/joint-statement-commissioners-noah-joshua-phillips-christine-s-wilson.

The Revised Safeguards Rule will require, within 30 days of Federal Register publication, covered companies to implement periodic risk assessments, modify their information security programs based in part on those risk assessments, and regularly test system controls and safeguards with more specific requirements. Additionally, within a year of Federal Register publication, the Revised Safeguards Rule will require covered companies to maintain written incident response plans and implement specific security requirements including multi-factor authentication, access controls, and encryption. In a separate supplemental notice of proposed rulemaking ("SNPRM"),[5] the FTC is also proposing to add reporting of security incidents to the FTC by covered companies within 30 days of discovery.

Altogether, the revised rule represents a more prescriptive regulatory approach similar to the New York Department of Financial Services' cybersecurity regulation,[6] and it will require more detailed compliance efforts by companies covered by GLBA including many Fintechs.

SCOPE OF FTC'S SAFEGUARDS RULE AND LATEST RULEMAKING

Congress directed the FTC to promulgate the Safeguards Rule through the passage of the Gramm-Leach-Bliley Act in 1999, and the Safeguards Rule was implemented in an effort to protect consumer financial information. The Revised Safeguards Rule largely covers the same financial institutions covered under the existing rule, including:

- Mortgage lenders and brokers;
- Payday lenders;
- Finance companies;
- Account servicers;
- Check cashers;
- Wire transferors;
- Travel agencies (when operated in connection with financial services);
- Collection agencies;
- Credit counselors and other financial advisors;

---

[5] https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-314-standards-safeguarding-customer-information-2.

[6] https://www.dfs.ny.gov/industry_guidance/cybersecurity.

- Tax preparation firms;
- Non-federally insured credit unions; and
- Investment advisors not required to register with the Securities and Exchange Commission.

The revised rule also covers entities acting as "finders" and exempts financial institutions with information on fewer than five thousand consumers from certain requirements.

The FTC announced proposed revisions to the Safeguards Rule through a request for public comment[7] in March 2019. In July 2020, the agency held a workshop[8] to examine the proposed changes to the Safeguards Rule. The workshop explored the practical application of the proposed revisions, as well as the costs and benefits to rule changes. The Revised Safeguards Rule adopts many of the proposals included in the 2019 request for comment and discussed at the workshop a year later. Some of those newly adopted proposals will take effect 30 days after Federal Register publication, while others will not be implemented until one year following publication.

RULES EFFECTIVE 30 DAYS AFTER PUBLICATION

The Revised Safeguards Rule requires covered financial institutions to, among other things, base their information security program on a periodic risk assessment and regular testing that is designed to detect actual and attempted attacks on, or intrusions into, information systems. Covered financial institutions are also required to modify their information security programs in accordance with periodic risk assessments.

RULES EFFECTIVE ONE YEAR AFTER PUBLICATION

Many additional security requirements go into effect one year after publication. For example, covered financial institutions will be required to:

- Require a "qualified individual" to oversee and implement the information security program;
- Require the designated "qualified individual" to regularly report in writing to the company board of directors or equivalent governing

---

[7] https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-314-standards-safeguarding-customer-information-0.

[8] https://www.ftc.gov/news-events/events-calendar/information-security-financial-institutions-ftc-workshop-examine.

body;

- Implement access controls, encryption, multi-factor authentication, retention and disposal policies, and logging;
- Establish periodic security assessments for service providers; and
- Create written incident response plans.

Additionally, the rules that will take effect one year after publication include more specific requirements for periodic risk assessments. Specifically, the risk assessment must: (1) evaluate the categorization of identified security risks that the financial institution faces; (2) assess the confidentiality, integrity, and availability of information systems and customer information; and (3) describe how the identified risks will either be mitigated or accepted based on the risk assessment, and how the financial institution's information security program will address the risks. The Revised Safeguards Rule also requires that regular testing include penetration testing and vulnerability assessments.

ADDITIONAL PROPOSED CHANGES

The FTC is also seeking comment on further changes to the rule through a supplemental notice of proposed rulemaking ("SNPRM").[9] Specifically, the SNPRM proposes to add reporting of security incidents to the FTC by covered financial institutions within 30 days of discovery. Additionally, the notification would include:

(1) the name and contact information of the company reporting the incident;

(2) a description of the type of information involved in the incident;

(3) if possible to determine, the date or timeline of the event; and

(4) a general description of the security event.

Comments on the SNPRM will be due 60 days after publication in the Federal Register.

In light of these changes, covered companies will need to closely evaluate their security practices for compliance, and should consider weighing in on incident reporting provisions that have been issued for comment.

---

[9] https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-314-standards-safeguarding-customer-information-2.