AN A.S. PRATT PUBLICATION
SEPTEMBER 2019
VOL. 5 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 7 SEPTEMBER 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
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 Web site ..... 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: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [209] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine 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 inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. 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 *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

SEC Warns Registered Firms about Client Privacy and Data Security

By Natasha G. Kohne, Michelle A. Reed, Peter I. Altman, Diana E. Schaffner, and Nicole Ashley Greenstein*

The authors of this article explain a Securities and Exchange Commission Office of Compliance Inspections and Examinations Risk Alert warning investment advisors and broker-dealers to review their policies and procedures regarding Regulation S-P, a privacy rule designed to safeguard customer records and information.

The Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert warning investment advisors and broker-dealers to review their policies and procedures regarding Regulation S-P ("Reg S-P"), a privacy rule designed to safeguard customer records and information that is also known as the Safeguards Rule and the Identity Theft Red Flags Rule.[1] OCIE issued the alert after seeing repeated deficiencies in Reg S-P compliance during examinations.

BACKGROUND

The SEC's latest Risk Alert comes on the heels of a recently announced enforcement action regarding Reg S-P, which resulted in a $1 million fine for failed policies and procedures that resulted in a breach.[2] The SEC's recent Risk Alert continues the recent emphasis on Reg S-P and cybersecurity and data privacy generally. The SEC details two key requirements of Reg S-P: privacy and opt-out notices and written policies and procedures.

- *Privacy and Opt-Out Notices*: Reg S-P requires a firm to provide a "clear and conspicuous notice" to customers that accurately reflects the firm's privacy

* Natasha G. Kohne (nkohne@akingump.com) is a partner at Akin Gump Strauss Hauer & Feld LLP and co-leader of the firm's cybersecurity, privacy, and data protection practice focusing on investigations, litigation, regulatory, and compliance. Michelle A. Reed (mreed@akingump.com) is a partner at the firm and co-leader of the firm's cybersecurity, privacy, and data protection practice focusing civil litigation, with an emphasis on securities and consumer class actions, as well as internal investigations. Peter I. Altman (paltman@akingump.com), a partner at the firm, represents investment management firms, private and public companies, and individuals in white collar and other government enforcement and regulatory matters, securities class litigation, and internal investigations. Diana E. Schaffner (dschaffner@akingump.com) is counsel at the firm advising clients on privacy- and cybersecurity-related litigation, investigations, and enforcement actions. Nicole Ashley Greenstein (ngreenstein@akingump.com) is an associate at the firm handling commercial litigation and advising on regulatory and compliance matters.

[1] https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

[2] https://www.sec.gov/news/press-release/2018-213.

policies and practices upon establishing a customer relationship ("Initial Privacy Notice"),[3] as well as not less than annually throughout the customer relationship ("Annual Privacy Notice").[4] It also requires a firm to deliver a "clear and conspicuous notice" to customers that accurately explains the right to opt out of some disclosures of the customer's non-public personal information to third parties ("Opt-Out Notice").[5] Reg S-P provides clear guidance on what should be included in these notices. Use of the SEC's model notice form provides a "safe harbor" from claims related to the privacy notice.[6]

- *Written Policies and Procedures to Safeguard Customer Information*: Reg S-P's Safeguard Rule requires firms to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[7] Policies and procedures must be reasonably designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

COMMON COMPLIANCE ISSUES

OCIE listed the most common deficiencies regarding Reg S-P that its staff discovered during examinations. These deficiencies fell into three categories: (1) privacy and opt-out notices; (2) a lack of policies and procedures; and (3) policies that were not implemented or not reasonably designed to safeguard customer records and information.

Privacy and Opt-Out Notices

OCIE staff observed firms that did not provide Initial Privacy Notices, Annual Privacy Notices, and Opt-Out Notices to their customers. Some firms provided notices that did not accurately reflect the firm's policies and procedures. Firms should ensure that they are regularly providing customers with all privacy notices and opt-out notices required by Reg S-P and that these notices accurately reflect the firm's policies and procedures.

[3] 17 CFR § 248.4.
[4] 17 CFR § 248.5.
[5] 17 CFR § 248.7.
[6] 17 CFR § 248.2.
[7] 17 CFR 248.30(a).

Lack of Policies and Procedures

OCIE staff also discovered some firms still do not have written policies and procedures as required by the Safeguards Rule. Some firms simply restated the Safeguards Rule, without including policies and procedures related to administrative, technical, and physical safeguards. A firm's policies and procedures must do more than simply address the delivery and content of a Privacy Notice to comply with the Safeguards Rule. OCIE also found firms with written policies and procedures that "contained numerous blank spaces designed to be filled in by registrants." Firms should ensure that they have comprehensive policies and procedures in place that address administrative, technical, and physical safeguards, as required by Reg S-P. These policies and procedures should be specifically tailored to the firm, rather than generic, boilerplate provisions.

Policies Not Implemented or Not Reasonably Designed to Safeguard Customer Records and Information

OCIE staff observed firms with written policies and procedures that did not comply with the Safeguard Rule inasmuch as they either were not implemented or were not reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to customers.

To comply with the Safeguard Rule, a firm's policies and procedures should be comprehensive. The following are a few key areas that OCIE highlighted in the recent alert that should be covered in a firm's policies and procedures.

- *Outside Vendors*: Adopt and implement strong policies and procedures concerning outside vendors that require vendors to meet certain security benchmarks. Monitor your vendors to ensure they comply with their contractual obligations.
- *PII Inventory*: Inventory all systems on which the firm maintains customer personally identifiable information ("PII"). Ensure policies and procedures account for the results of this inventory.
- *Incident Response Plans*: Adopt, implement and test written incident response plans that provide real-life guidance to facilitate quick plan implementation and that take into account known system vulnerabilities.
- *Personal Devices*: Adopt and implement policies and procedures to safeguard customer information on personal devices (personal laptops, smartphones, iPads, etc.) and explain the same to employees.

- *Training and Monitoring*: Train employees on encryption, password protection and other security measures. Regularly test employees through routine fake phishing exercises and similar activities to ensure compliance.

CONCLUSION

The OCIE alert serves as a warning to firms to avoid the same mistakes that others have repeatedly made over the last two years. SEC-registered firms should carefully review their written policies and procedures, as well as how these policies and procedures are implemented, to ensure full compliance with Reg S-P. At a minimum, firms should ensure that: (1) they provide customers with initial and annual privacy notices, as well as opt-out notices, that actually reflect their policies and procedures; (2) they have written policies and procedures related to administrative, technical and physical safeguards; and (3) their policies are implemented and reasonably designed to safeguard customer records and information.