AN A.S. PRATT PUBLICATION
MAY 2023
VOL. 9 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 4** **May 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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, 631.291.5541. 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.

New York State Department of Financial Services Proposes More Changes to Its Cybersecurity Requirements

By Scott D. Samlin and Daniel V. Funaro*

In this article, the authors discuss a second amendment proposed by the New York State Department of Financial Services to its Cybersecurity Requirements for Financial Services Companies.

The New York State Department of Financial Services (NYDFS) has released its proposed second amendment to its Cybersecurity Requirements for Financial Services Companies (Part 500), which includes heightened cybersecurity requirements for some companies, new security event reporting requirements, and mandated multi-factor authentication for remo te access to systems. The newly proposed amendment follows up on the NYDFS' pre-proposal outreach from earlier last year.

CLASS A COMPANIES

Foremost among the proposed changes is the creation of a separate category of regulated entity known as "Class A Companies." Previously, Part 500 regulations have applied uniformly to all non-exempt entities operating under New York banking, insurance, or financial services law licenses, registrations, or authorizations.

The proposed amendments include a heightened set of requirements for Class A Companies, which are defined as entities with at least $20 million in gross annual revenue in each of the last two fiscal years from New York business operations and either (1) greater than 2,000 employees (including employees of affiliates) averaged over the last two fiscal years, wherever located, or (2) greater than $1 billion in gross annual revenue (including revenue from affiliates) in each of the last two fiscal years from all business operations, wherever located.

Among the heightened requirements specifically applicable to Class A Companies are the following:

1. Performing, at minimum, annual independent audits of their cybersecurity systems;

---

* Scott D. Samlin, a partner in the New York office of Blank Rome LLP, focuses his practice on representing financial institutions, corporations, and other entities in mortgage banking and consumer financial services issues. Daniel V. Funaro, an associate in the firm's office in Washington, D.C., concentrates his practice on advising consumer and commercial financial services providers on regulatory compliance issues, including compliance with state and federal regulations and state licensing regimes. The authors may be contacted at scott.samlin@blankrome.com and daniel.funaro@blankrome.com, respectively.

2. Blocking weak or commonly used passwords for all accounts that use company systems (or implementing a similar system with compensating controls);

3. Hiring external experts to conduct a cybersecurity risk assessment at least once every three years;

4. Implementing an endpoint detection and response solution to monitor anomalous cybersecurity-related activity including lateral movement; and

5. Implementing a centralized system for security event logging and alerting.

Additional proposed changes found in the amendment include annual penetration testing obligations and requirements related to implementing monitoring processes to ensure prompt notification of new security vulnerabilities, maintaining written policies and procedures for vulnerability management and conducting automated vulnerability scans, and reviewing and updating risk assessments annually.

Significantly, covered entities will need to utilize multi-factor authentication for all those with remote access to either the entity's information systems or third-party applications, including but not limited to those that are cloud based, from which nonpublic information is available. So-called "Privileged Accounts" (accounts that perform security-relevant functions that ordinary users are not authorized to perform or that can affect material changes to the technical or business operations of the covered entity) will also need to use multi-factor authentication.

NEW SECURITY EVENTS

Finally, the proposed amendment also defines three new security events that must be reported to the NYDFS within 72 hours:

1. Unauthorized access to Privileged Accounts,

2. Deployment of ransomware within a material part of a covered entity's systems, and

3. Any cybersecurity event affecting a third-party service provider that also affects the covered entity.

CONCLUSION

After the final amendments are released, they will become effective upon publication of the Notice of Adoption in the New York State Register, but covered entities will have a transition period ranging between 30 days and two years to come into compliance with most of the updated provisions.