

AN A.S. PRATT PUBLICATION  
NOVEMBER-DECEMBER 2020  
VOL. 6 • NO. 9

PRATT'S  
**PRIVACY &  
CYBERSECURITY  
LAW**  
REPORT



LexisNexis

**EDITOR'S NOTE: INITIATIVES**

Victoria Prussen Spears

**CYBERSECURITY PREPAREDNESS AND  
THE GROWING IMPORTANCE OF  
OPERATIONAL RESILIENCY**

Brian E. Finch, Cassandra Lentchner, and  
David Oliwenstein

**U.S. SENATORS INTRODUCE BILL  
IMPOSING STRINGENT, NATIONAL  
BIOMETRIC PRIVACY REGULATION**

Jeffrey N. Rosenthal and David J. Oberly

**THE CALIFORNIA PRIVACY RIGHTS  
ACT HAS PASSED: WHAT'S IN IT?**

Brandon P. Reilly and Scott T. Lashway

**THE DAWNING OF NYDFS  
CYBERSECURITY REGULATION  
ENFORCEMENT**

Jami Mills Vibbert, Michael A. Mancusi,  
Nancy L. Perkins, Alex Altman,  
Anthony Raglani, Javier Ortega, and  
Kevin M. Toomey

**SCHREMS STRIKES AGAIN: BATTERY OF  
NEW DATA PRIVACY COMPLAINTS RAISE  
COMPLIANCE QUESTIONS FOR EU-U.S.  
DATA TRANSFERS**

Angelo A. Stio III, Sharon R. Klein, and  
Jason J. Moreira

**DESIGNING A BIPA DEFENSE: USING  
PREEMPTION AND ARBITRATION TO  
DEFEAT BIOMETRIC CLASS ACTIONS**

Jeffrey N. Rosenthal and David J. Oberly

# Pratt's Privacy & Cybersecurity Law Report

---

---

VOLUME 6

NUMBER 9

NOVEMBER - DECEMBER 2020

---

**Editor's Note: Initiatives**

Victoria Prussen Spears 265

**Cybersecurity Preparedness and the Growing Importance of  
Operational Resiliency**

Brian E. Finch, Cassandra Lentchner, and David Oliwenstein 267

**U.S. Senators Introduce Bill Imposing Stringent,  
National Biometric Privacy Regulation**

Jeffrey N. Rosenthal and David J. Oberly 272

**The California Privacy Rights Act Has Passed: What's In It?**

Brandon P. Reilly and Scott T. Lashway 276

**The Dawning of NYDFS Cybersecurity Regulation Enforcement**

Jami Mills Vibbert, Michael A. Mancusi, Nancy L. Perkins, Alex Altman,  
Anthony Raglani, Javier Ortega, and Kevin M. Toomey 285

**Schrems Strikes Again: Battery of New Data Privacy Complaints Raise  
Compliance Questions for EU-U.S. Data Transfers**

Angelo A. Stio III, Sharon R. Klein, and Jason J. Moreira 288

**Designing a BIPA Defense: Using Preemption and Arbitration to  
Defeat Biometric Class Actions**

Jeffrey N. Rosenthal and David J. Oberly 292

## 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 [245] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2020 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

*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](http://www.lexisnexis.com)

MATTHEW  BENDER

(2020-Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

---

## **EDITOR-IN-CHIEF**

**STEVEN A. MEYEROWITZ**

*President, Meyerowitz Communications Inc.*

## **EDITOR**

**VICTORIA PRUSSEN SPEARS**

*Senior Vice President, Meyerowitz Communications Inc.*

## **BOARD OF EDITORS**

**EMILIO W. CIVIDANES**

*Partner, Venable LLP*

**CHRISTOPHER G. CWALINA**

*Partner, Holland & Knight LLP*

**RICHARD D. HARRIS**

*Partner, Day Pitney LLP*

**JAY D. KENISBERG**

*Senior Counsel, Rivkin Radler LLP*

**DAVID C. LASHWAY**

*Partner, Baker & McKenzie LLP*

**CRAIG A. NEWMAN**

*Partner, Patterson Belknap Webb & Tyler LLP*

**ALAN CHARLES RAUL**

*Partner, Sidley Austin LLP*

**RANDI SINGER**

*Partner, Weil, Gotshal & Manges LLP*

**JOHN P. TOMASZEWSKI**

*Senior Counsel, Seyfarth Shaw LLP*

**TODD G. VARE**

*Partner, Barnes & Thornburg LLP*

**THOMAS F. ZYCH**

*Partner, Thompson Hine*

---

*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. Copyright 2020 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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.

# The Dawning of NYDFS Cybersecurity Regulation Enforcement

*By Jami Mills Vibbert, Michael A. Mancusi, Nancy L. Perkins, Alex Altman, Anthony Raglani, Javier Ortega, and Kevin M. Toomey \**

*The authors of this article discuss an enforcement action under New York's Cybersecurity Requirements for Financial Services Companies.*

The New York Department of Financial Services (“NYDFS”) has commenced its first enforcement action under New York’s Cybersecurity Requirements for Financial Services Companies.<sup>1</sup> Part 500, which requires financial institutions subject to NYDFS jurisdiction to establish and maintain certain cybersecurity standards to protect Nonpublic Information (“NPI”) within their control, has been described as a “first in the nation” regulation due to its detailed cybersecurity obligations. NYDFS has prioritized compliance with Part 500 in regular and targeted examinations of NYDFS-supervised institutions, and now has taken the next step in an enforcement action against First American Title Insurance Company.

## BACKGROUND

Part 500 took effect in 2017 and was fully implemented as of March 2019. Pursuant to its mandates, entities under NYDFS jurisdiction must implement appropriate cybersecurity policies and procedures based on risk assessments for NPI, which because of its inclusion of certain business-related information is quite broad and unlike many other data protection standards. Effective controls, employee training, and good governance are also required.

## THE NEW ACTION

In a Statement of Charges and Notice of Hearing,<sup>2</sup> the NYDFS alleges that First American – the second largest title insurance provider in the United States, handling millions of documents containing sensitive personal information – violated numerous Part 500 requirements.

---

\* Jami Mills Vibbert (jami.vibbert@arnoldporter.com) and Michael A. Mancusi (michael.mancusi@arnoldporter.com) are partners and Nancy L. Perkins (nancy.perkins@arnoldporter.com) is counsel at Arnold & Porter Kaye Scholer LLP. Alex Altman (alexander.altman@arnoldporter.com), Anthony Raglani (anthony.raglani@arnoldporter.com) and Kevin M. Toomey (kevin.toomey@arnoldporter.com) are senior associates and Javier Ortega (javier.ortega@arnoldporter.com) is an associate at the firm.

<sup>1</sup> 23 NYCRR Part 500.

<sup>2</sup> [https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721\\_first\\_american\\_notice\\_charges.pdf](https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf).

Among other things, the Notice alleges that First American failed to address a known vulnerability in its document-handling program, exposing millions of documents containing NPI. Although it is still unclear how many documents were exposed, by its own analysis, First American identified that, in an 11-month period, approximately 350,000 documents that should have been restricted were accessed by automated programs scraping the internet.

The Notice states that the NYDFS determined that First American had stored documents used to obtain title insurance (many of which contain NPI such as Social Security numbers and financial account information) in a proprietary document management system known as FAST.

According to the Notice, in order to share documents stored in FAST with title agents or parties to a real estate transaction, First American implemented EaglePro, a web-based title document delivery system. Documents in EaglePro allegedly were accessible through a website link shared by parties to a transaction with each other.

Because documents in EaglePro were sequentially numbered and users were not required to verify their identities, any person – including unauthorized individuals – with an EaglePro link allegedly could change a number in the URL to access other documents available through the platform. Unauthorized individuals could also find and view documents containing NPI in Google search results. As of 2019, website links did not have expiration dates.

The Company's Cyber Defense Team discovered this vulnerability in December 2018 and quickly alerted the EaglePro Application Development Team. The Cyber Defense Team issued a report in January 2019 describing the vulnerability, but according to the Notice, the Company did not take steps to remediate the vulnerability for at least six months thereafter.

## **ALLEGED CYBERSECURITY FAILURES**

The NYDFS Notice describes First American's response to the EaglePro vulnerability as "a cascade of errors." The alleged errors include:

- Failing to follow its own cybersecurity policies by not performing a risk assessment or a security review of EaglePro;
- Underestimating the level of risk associated with the EaglePro vulnerability by internally classifying it as "medium severity," due to its mistaken belief that EaglePro could not transmit NPI;
- Delaying addressing the vulnerability because of a subsequent misclassification as a "low severity" vulnerability due to an administrative error;

- Failing to conduct further risk assessments against the advice of the Cyber Security Defense Team;
- Failing to follow its own internal policies and controls to address the EaglePro vulnerability;
- Assigning an unqualified and uninformed employee with little experience in data security to fix the vulnerability; and
- Maintaining an inadequate manual process subject to human error for identifying documents with NPI, compounded by insufficient training.

The Notice stresses, as a central allegation, that First American not only “lacked adequate controls” to protect NPI, but also failed to conduct an adequate risk assessment.

### **CONSIDERATIONS**

The NYDFS’s new enforcement action clearly underscores that, to comply with Part 500, covered entities must conduct thorough risk assessments and promptly institute controls sufficient to address identified cybersecurity vulnerabilities. The risk assessment requirement is a cornerstone of Part 500 and should serve as the basis upon which covered entities’ cybersecurity programs and policies are developed and maintained.

Without a thorough and meaningful risk assessment, based on legal standards such as those contained in Part 500, a covered entity is unlikely to identify and implement the risk-based controls required to protect its information systems and NPI or to effectively identify vulnerabilities that should be remediated.

The enforcement action thus serves as a lesson for industry participants to not only take care in developing compliant cybersecurity programs, but to ensure that such programs are properly implemented and continually reevaluated through self-testing.