

AN A.S. PRATT PUBLICATION

OCTOBER 2026

VOL. 12 NO. 8

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



LexisNexis

EDITOR'S NOTE: PRIVACY IN THE STATES

Victoria Prussen Spears

**DELAWARE'S PRIVACY LAW IS ABOUT
TO EXPAND: 6 STEPS EMPLOYERS AND
BUSINESSES SHOULD TAKE TO PREPARE**

Vivian Isaboke

**OKLAHOMA ENACTS NATION'S TWENTIETH
STATE COMPREHENSIVE PRIVACY LAW**

Kirk J. Nahra, Ali A. Jessani and
Blythe Riggan

**ALABAMA ENACTS NATION'S TWENTY-FIRST
STATE COMPREHENSIVE PRIVACY LAW**

Kirk J. Nahra, Samuel Kane and Blythe Riggan

**NEW YORK STATE DEPARTMENT OF FINANCIAL
SERVICES RAMPS UP HEALTH CARE CYBERSECURITY
ENFORCEMENT WITH \$2.25 MILLION SETTLEMENT**

Jason Johnson and Linda Malek

**THE GOOD, THE BAD, AND THE UGLY: WHAT 7
RECENT COURT DECISIONS TELL YOU ABOUT
TODAY'S WEBSITE PRIVACY LIABILITY**

Usama Kahf

**CHARTING NEW WATERS: ENGLISH HIGH COURT
CONFINES EFFECT OF *THREE RIVERS (NO 5)*,
CONFIRMING PRIVILEGE CAN APPLY TO
INTRA-CLIENT COMMUNICATIONS**

James Norris-Jones and Tim Vogel

**COURT OF JUSTICE OF THE EUROPEAN UNION
RULES THAT A FIRST DATA SUBJECT ACCESS
REQUEST CAN BE REFUSED AS EXCESSIVE**

Huw Beverley-Smith, Charlotte H N Perowne
and James Ford

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12

NUMBER 8

October 2026

Editor's Note: Privacy in the States Victoria Prussen Spears	255
Delaware's Privacy Law Is About to Expand: 6 Steps Employers and Businesses Should Take to Prepare Vivian Isaboke	257
Oklahoma Enacts Nation's Twentieth State Comprehensive Privacy Law Kirk J. Nahra, Ali A. Jessani and Blythe Riggan	264
Alabama Enacts Nation's Twenty-First State Comprehensive Privacy Law Kirk J. Nahra, Samuel Kane and Blythe Riggan	268
New York State Department of Financial Services Ramps Up Health Care Cybersecurity Enforcement With \$2.25 Million Settlement Jason Johnson and Linda Malek	273
The Good, the Bad, and the Ugly: What 7 Recent Court Decisions Tell You About Today's Website Privacy Liability Usama Kahf	277
Charting New Waters: English High Court Confines Effect of <i>Three Rivers (No 5)</i>, Confirming Privilege Can Apply to Intra-Client Communications James Norris-Jones and Tim Vogel	283
Court of Justice of the European Union Rules That a First Data Subject Access Request Can Be Refused as Excessive Huw Beverley-Smith, Charlotte H N Perowne and James Ford	288

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@lexisnexus.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
LexisNexis® Support Center <https://supportcenter.lexisnexus.com/app/home>
For information on other Matthew Bender publications, please call
Your account manager or (800) 223-1940
Outside the United States and Canada, please call (518) 487-3385

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*, [7] PRATT’S PRIVACY &
CYBERSECURITY LAW REPORT [179] (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 © 2026 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.lexisnexus.com

MATTHEW  BENDER

(2026–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, Sidley Austin 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 2026 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 inquiries 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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

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 Ramps Up Health Care Cybersecurity Enforcement With \$2.25 Million Settlement

*By Jason Johnson and Linda Malek**

In this article, the authors explore a recent cybersecurity settlement reached by the New York State Department of Financial Services with Delta Dental of New York and Delta Dental Insurance Co.

The New York State Department of Financial Services (NYDFS) recently announced the finalization of a \$2.25 million settlement¹ with Delta Dental of New York and Delta Dental Insurance Co., resolving allegations that the affiliated companies failed to comply with the state's stringent cybersecurity, consumer data protection, and incident reporting requirements. For health insurers, managed care organizations, and their third-party service providers operating in New York, the announcement comes as the latest signal that the NYDFS intends to aggressively enforce its cybersecurity regulations — which are widely considered the strictest in the nation following a 2023 overhaul.² These regulations, codified at 23 NYCRR 500 (Cybersecurity Requirements for Financial Services Organizations),³ apply to any entity licensed under New York insurance law, including health insurers, managed care organizations, and their third-party service providers.

This recent development both spotlights the enhanced compliance obligations payors operating in New York state face under the revamped NYDFS regulations *and* illustrates the importance of proactively developing, enacting, and communicating a comprehensive cybersecurity strategy that encompasses:

- A clear data retention policy that ensures timely disposal of plan members' nonpublic information (NPI).
- Detailed and actionable guidance for employees in the event of a cyber breach or other incident.

* The authors, partners in Crowell & Moring LLP, may be contacted at jjohnson@crowell.com and lmalek@crowell.com, respectively.

¹ <https://www.dfs.ny.gov/system/files/documents/2026/04/Delta-Dental-Consent-Order.pdf>.

² https://www.dfs.ny.gov/industry_guidance/cybersecurity.

³ https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

- Instructions for employees to comply with all state-level notice requirements (including disclosures to members and regulators) within statutory deadlines.
- Risk mitigation strategies and compliance best practices regarding the use of vendor tools and services.

ENFORCEMENT IN PERSPECTIVE: WHY THE DELTA DENTAL SETTLEMENT MATTERS

The Delta Dental investigation arose from a 2023 data breach in which hackers took advantage of a then-unknown flaw in MOVEit, a third-party file tool used by the organization to securely transfer data. The breach exposed approximately 60,000 files containing sensitive policyholder information, including Social Security numbers, financial details, and health records. Following a NYDFS investigation, regulators contended that the companies lacked adequate data disposal policies, failed to maintain sufficiently detailed incident response plans, and did not notify authorities until mid-December 2023 — a date well beyond the rule's required 72-hour reporting window. The matter was ultimately resolved through a consent order⁴ requiring a \$2.25 million payment; however, the underlying investigation provides invaluable insight into the NYDFS' enforcement strategy and potential compliance risks.

First, it should be noted that the Delta Dental matter is one of *two* multimillion-dollar resolutions pursued by the NYDFS against health care organizations alleged to have violated the state's robust cybersecurity requirements within the last calendar year. In August 2025, the NYDFS resolved an action⁵ against Healthplex, Inc., a dental insurance management services company licensed as an independent adjuster and insurance agent, following allegations that its inadequate cybersecurity protocols — and, in particular, its alleged failure to fully implement multi-factor authentication (MFA) safeguards — contributed to the exposure of customer data after a 2021 phishing attack.

Second, the investigation illustrates that HIPAA compliance *does not* satisfy a payor's full cybersecurity obligations under New York law. The Delta Dental matter focused in part on alleged violations of Section 500.13 of 23 NYCRR 500,⁶ which requires covered entities to establish policies and procedures for the secure disposal of nonpublic information that is no longer necessary for business operations. This is a data minimization standard more commonly associated with privacy law than with HIPAA, which focuses primarily on limiting access to and disclosure of data rather than

⁴ <https://www.dfs.ny.gov/system/files/documents/2026/04/Delta-Dental-Consent-Order.pdf>.

⁵ https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250814.

⁶ https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

mandating deletion. Organizations that have built their compliance programs around HIPAA alone may be leaving a significant gap with respect to this deletion obligation — one that the NYDFS appears to be actively closing through enforcement.

Third, it is worth noting that both the Delta Dental and Healthplex matters are among the first enforcement actions brought against health care organizations in the period following the amendment of 23 NYCRR 500. Importantly, however, both enforcement actions were brought under the version of the regulations that predated the November 2023 amendments⁷ — meaning even the pre-amendment obligations are being actively enforced. The final phase of new requirements took effect in November 2025, imposing new obligations regarding:

- *Multi-factor authentication (MFA)*. The updated regulations now require MFA for all individuals accessing any of a covered entity's information systems, applying without distinction as to where a user is located, what role they hold, or what category of data happens to reside on the system in question. Entities that qualify for the limited exemption under Section 500.19(a) face a narrower but still significant obligation: MFA must be in place for remote access to the covered entity's own systems, access to outside applications — including those hosted in the cloud — that handle nonpublic information, and all elevated-privilege accounts, with the exception of service accounts that do not permit interactive login. As artificial intelligence tools become more deeply integrated into payor operations, the breadth of this obligation is likely to expand accordingly.
- *Asset inventory*. Covered entities must now formalize and maintain a formal, well-documented record of all information systems within the organization, supported by written procedures that address how asset details are captured and how often the inventory is reviewed and confirmed as current.

Finally, organizations should be aware that the NYDFS has made clear it *will not* permit responsibility for cybersecurity compliance to be delegated to vendors. In an October 2025 guidance,⁸ NYDFS signaled that it will hold covered organizations (defined in 23 NYCRR 500⁹ as “any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law”) accountable when vendor oversight is inadequate, treating such gaps as relevant considerations in regulatory reviews and disciplinary proceedings.

⁷ https://www.dfs.ny.gov/system/files/documents/2023/11/cybersecurity_implementation_timeline_covered_entities.pdf.

⁸ <https://www.dfs.ny.gov/industry-guidance/industry-letters/il20251021-guidance-managing-risks-third-party>.

⁹ https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

IMPLICATIONS AND RECOMMENDATIONS FOR PAYORS

The Delta Dental settlement, taken in conjunction with recent NYDFS communications and the 2025 Healthplex action, makes it clear that the NYDFS views cybersecurity enforcement in the health care and insurance sectors as an ongoing priority — and that compliance with the amended 23 NYCRR 500 requirements will be closely scrutinized. Health insurers and managed care organizations operating in New York should treat these enforcement actions not merely as cautionary tales, but as a roadmap for the compliance gaps regulators are most likely to target, including data disposal practices, incident response planning, vendor oversight, and MFA implementation.

Health insurers and managed care organizations should assess and strengthen their cybersecurity compliance programs, evaluate vendor due diligence practices, and align privacy and security policies with NYDFS requirements. Proactive engagement with these obligations, rather than reactive remediation following a breach or regulatory inquiry, remains the most effective strategy for managing enforcement risk under New York's increasingly rigorous cybersecurity framework.