AN A.S. PRATT PUBLICATION
JUNE 2025
VOL. 11 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 5** **June 2025**

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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.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)

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

(2025–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 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.

Lessons from PayPal's $2 Million Cybersecurity Settlement with the New York State Department of Financial Services

By Craig R. Heeren*

In this article, the author reviews PayPal's recent settlement with the New York State Department of Financial Services, explaining that it highlights the importance of implementing an effective cybersecurity program and ensuring that employees are adequately trained to follow the policy in practice.

PayPal has settled an enforcement action brought by the New York State Department of Financial Services (NYDFS) for failing to comply with cybersecurity regulations required for financial services businesses under the NYDFS's supervision. The settlement, which included a $2 million fine and required remedial measures, arose out of a cybersecurity incident where hackers gained access to PayPal customers' sensitive information contained on tax forms in PayPal's systems. As discussed further below, the incident highlights the importance of implementing an effective cybersecurity program and ensuring that employees are adequately trained to follow the policy in practice.

SUMMARY OF THE PAYPAL ENFORCEMENT DECISION

The NYDFS sets standards for cybersecurity practices among financial institutions through cybersecurity regulations established at 23 NYCRR Part 500. These regulations require all DFS-regulated entities to establish and maintain a comprehensive cybersecurity program to protect consumers' nonpublic information (NPI) and ensure the security of information systems.

The Incident

The NYDFS's investigation into PayPal's cybersecurity practices was triggered by a cybersecurity incident that occurred in December 2022. Due to changes in federal tax laws, PayPal amended its systems to provide more customers with "Form 1099-Ks," which contain sensitive information such as Social Security numbers (SSNs), names, and dates of birth. One day after the new system was implemented, threat actors exploited a vulnerability allowing them to gain unauthorized access to accounts through a "credential-stuffing" scheme. Once in the account, they were able to access unmasked (i.e., not encrypted, anonymized or otherwise shielded from view) customer data contained in the Form 1099-Ks. PayPal stopped the attack by adding CAPTCHA and rate-limiting and remediated the harm by masking the data and enforcing account resets on impacted accounts.

* The author, a partner in the New York office of Faegre Drinker Biddle & Reath LLP, may be contacted at craig.heeren@faegredrinker.com.

The Cause of the Incident and NYDFS Conclusions

NYDFS concluded that the incident was caused by a combination of factors. Although PayPal had an existing policy (the Risk and Control Identification Process) designed to ensure that they analyze and test any product changes for cybersecurity vulnerabilities, the team implementing the 1099-K change was not adequately trained on the application of this policy. As a result, they misclassified the change, and no analysis or testing under the policy was performed on the new 1099-K process, which might have identified that the data was unmasked and that a security vulnerability existed that provided unauthorized access.

Additionally, although PayPal had a policy that all account information be protected through "risk-based authentication," the company permitted multi-factor authentication (MFA) to be optional for accounts. Mandatory MFA would have frustrated the ability to gain access to accounts by the threat actors.

NYDFS identified three key violations of the Cybersecurity Regulations, alleging the following:

1. Inadequate Implementation of Cybersecurity Policies: PayPal failed to properly implement its own cybersecurity policies and procedures, particularly those related to access controls, identity management, and customer data privacy, in violation of 23 NYCRR §§ 500.3(d), (i), and (k).

2. Unqualified Cybersecurity Personnel: PayPal did not utilize qualified cybersecurity personnel to oversee and perform core cybersecurity functions, nor did it provide adequate training to its personnel, in violation of 23 NYCRR § 500.10(a).

3. Ineffective Access Controls: PayPal failed to use effective controls, such as mandatory Multi-Factor Authentication (MFA), to prevent unauthorized access to NPI, as required by 23 NYCRR § 500.12(a).

PayPal's Fine and Remediation

To resolve the matter. PayPal agreed to pay a $2 million fine and implement several remedial measures, including the following:

- Masking exposed NPI and implementing CAPTCHA to prevent automated account access.

- Updating policies to ensure clarity on when Risk and Control Identification Process (RCIP) applies.

- Providing comprehensive training to its engineering team on deploying code and enforcing RCIP.

- Requiring MFA for all U.S. customer account logins.

Notably, NYDFS identified PayPal's cooperation during the investigation and efforts to promptly remediate the identified issues as important factors in their settlement decision.

TAKEAWAYS

Several lessons can be learned from this action, discussed below.

Paper Compliance Versus Effective Compliance

The enforcement action against PayPal underscores the critical importance of not just creating, but effectively implementing and maintaining comprehensive cybersecurity policies and procedures that are consistent with the expectations of your regulator. Although PayPal had an existing cybersecurity policy, the failure by the relevant employees to follow that policy effectively rendered its protections irrelevant. Entities must ensure not only that they have written thoughtful, risk-based cybersecurity policies, but that their employees are properly trained and consistently follow those policies in their daily work.

Training Qualified Cybersecurity Personnel

The case highlights how simple user error – in this case incorrectly designating the type of work being conducted – can lead to a serious cybersecurity incident. Rigorous and continuous training for staff on the cybersecurity policies relevant to their job is the best defense against human error like what occurred here.

Additionally, employing competent cybersecurity personnel in supervisory roles may also help "issue-spot" errors by employees who are not as familiar with proper data handling and effective cybersecurity practices.

Implementation of Effective Access Controls

The failure to use mandatory MFA was a significant factor in the unauthorized access to PayPal's systems. Financial institutions should prioritize the implementation of effective access controls, such as MFA, to safeguard sensitive consumer information and prevent unauthorized access.

Timely and Proactive Remediation

PayPal's prompt response to the cybersecurity event, including masking exposed NPI and enforcing CAPTCHA, demonstrates the importance of timely and proactive remediation efforts. Organizations must be prepared to act swiftly in the event of a cybersecurity incident to mitigate potential damage, restore security, and maintain or gain credibility with government regulators and investigators.

Cooperation with Regulatory Authorities

Although the details are limited, NYDFS's discussion of PayPal's "commendable cooperation" indicates that efforts to work closely with the regulator likely led to a more

favorable settlement than might otherwise have occurred. Companies should evaluate, both as a general policy and after a particular cybersecurity incident, how they will approach an investigation by a regulator like NYDFS to ensure they receive credit for cooperation.