

AN A.S. PRATT PUBLICATION
NOVEMBER - DECEMBER 2022
VOL. 8 NO. 9

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



LexisNexis

EDITOR'S NOTE: KNOCK, KNOCK

Victoria Prussen Spears

**SEARCH WARRANTS: THE CRISIS DELIVERED
DIRECTLY TO YOUR FRONT DOOR**

Jason P. Bologna

**PREPARE NOW TO MANAGE YOUR WORKFORCE
THROUGH A CYBERATTACK**

Brian M. Noh

**CYBERSECURITY INSURANCE AND MANAGING
RISK: 10 THINGS TO KNOW**

Seth Harrington, Kelly Hagedorn and Cameron Carr

**COLORADO ATTORNEY GENERAL'S OFFICE
ISSUES DRAFT COLORADO PRIVACY ACT
REGULATIONS**

David P. Saunders, Cathy Lee, Amy C. Pimentel and
Elliot R. Golding

**WHAT PERSONAL INFORMATION ACCESS RIGHTS
WILL CALIFORNIA EMPLOYEES HAVE UNDER THE
CALIFORNIA PRIVACY RIGHTS ACT STARTING
JANUARY 1, 2023?**

Kristen J. Mathews, Suhna Pierce and Bela Karmel

**FIRST CALIFORNIA CONSUMER PRIVACY ACT
ENFORCEMENT ACTION SETTLEMENT AND
SUNSETTING OF EMPLOYEE DATA EXEMPTIONS
SIGNAL SIGNIFICANT COMPLIANCE CHALLENGES
AHEAD**

Alex C. Nisenbaum, Sharon R. Klein, Ana Tagvoryan
and Karen H. Shin

**THIRD CIRCUIT COURT OF APPEALS GIVES
PENNSYLVANIA CONSUMERS NEW FOOTING FOR
INTERNET TRACKING CLAIMS**

Thomas R. DeCesar and Jonathan R. Vaitl

**NEW YORK STATE DEPARTMENT OF FINANCIAL
SERVICES PENALIZES CRUISE SHIP OPERATOR
FOR FAILING TO PREVENT AND TIMELY REPORT
CYBERATTACKS**

Celeste Koeleveld, Daniel Silver and Megan Gordon

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8

NUMBER 9

November - December 2022

Editor's Note: Knock, Knock

Victoria Prussen Spears

295

Search Warrants: The Crisis Delivered Directly to Your Front Door

Jason P. Bologna

297

Prepare Now to Manage Your Workforce Through a Cyberattack

Brian M. Noh

300

Cybersecurity Insurance and Managing Risk: 10 Things to Know

Seth Harrington, Kelly Hagedorn and Cameron Carr

303

Colorado Attorney General's Office Issues Draft Colorado Privacy Act Regulations

David P. Saunders, Cathy Lee, Amy C. Pimentel and Elliot R. Golding

307

What Personal Information Access Rights Will California Employees Have Under the California Privacy Rights Act Starting January 1, 2023?

Kristen J. Mathews, Suhna Pierce and Bela Karmel

312

First California Consumer Privacy Act Enforcement Action Settlement and Sunsetting of Employee Data Exemptions Signal Significant Compliance Challenges Ahead

Alex C. Nisenbaum, Sharon R. Klein, Ana Tagvoryan and Karen H. Shin

315

Third Circuit Court of Appeals Gives Pennsylvania Consumers New Footing for Internet Tracking Claims

Thomas R. DeCesar and Jonathan R. Vaitl

320

New York State Department of Financial Services Penalizes Cruise Ship Operator for Failing to Prevent and Timely Report Cyberattacks

Celeste Koeleveld, Daniel Silver and Megan Gordon

323

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*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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 © 2022 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

MATTHEW  BENDER

(2022-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 2022 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, 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 Penalizes Cruise Ship Operator for Failing to Prevent and Timely Report Cyberattacks

*By Celeste Koeleveld, Daniel Silver and Megan Gordon**

In this article, the authors discuss a recent settlement between a cruise ship operator and New York regulators over an alleged cybersecurity breach.

The New York State Department of Financial Services (“NYDFS”) has issued a consent order (the “Order”) finding that cruise ship operator Carnival Corporation violated the department’s cybersecurity regulation by failing to implement required policies and procedures as well as report several cyber incidents that the company experienced. The enforcement action signals DFS’s determination to ensure all licensed entities – including victims of cyberattacks – fully protect sensitive customer and employee data by rigorously adhering to NYDFS’s cybersecurity regulation.

KEY ISSUES

- NYDFS found that Carnival Corporation violated the department’s cybersecurity regulation.
- The cruise line is under the purview of the agency via its insurance business.
- DFS licensees may be subject to penalties for cyber breaches and failure to protect sensitive data even if financial services comprise only a small portion of their overall operations.

OVERVIEW OF THE NYDFS CYBERSECURITY REGULATION

Adopted in March 2017, the NYDFS Cybersecurity Requirements for Financial Services Companies (the “Regulation”) require “Covered Entities” – including banks, insurance companies, and other institutions licensed or regulated by NYDFS, along with third-party service providers – to put in place a risk-based cybersecurity program that provides appropriate protection of the entity’s information systems and data. This

* Celeste Koeleveld, a partner in the New York office of Clifford Chance, represents clients with regulatory compliance, internal investigations, and all phases of civil, criminal and regulatory litigation. Daniel Silver, a partner in the firm’s New York office, focuses on regulatory enforcement and white collar criminal defense matters. Megan Gordon, the office managing partner for the firm’s Washington, D.C. office, focuses her practice on risk management, transactional due diligence, compliance and internal investigation matters. The authors may be contacted at celeste.koeleveld@cliffordchance.com, daniel.silver@cliffordchance.com and megan.gordon@cliffordchance.com, respectively.

program must include written policies and procedures, risk assessment activities, and other industry-standard cybersecurity program elements.

One such control emphasized by the Regulation is the use of multi-factor authentication (“MFA”), a requirement that is only excused when the chief information security officer (“CISO”) “approve[s] in writing the use of . . . reasonably equivalent or more secure access controls.” The CISO must also certify annually to NYDFS that the Covered Entity’s program is compliant and maintain supporting documentation for five years for examination by the regulator.

THE CARNIVAL CONSENT ORDER

NYDFS’s Consent Order discussed four cybersecurity incidents affecting Carnival Corporation that exposed customer and employee personal information. While Carnival Corporation’s primary business is operating cruise ships, it also offers life, accident, and health insurance pursuant to a license from NYDFS – activities that brought it within the scope of the Regulation. Most of the incidents arose from various ransomware attacks whereby hackers infiltrated Carnival’s information system through phishing emails sent to and from company email accounts.¹

According to the Order, Carnival became aware of the first cyber incident after an internal investigation revealed that unauthorized parties had gained access to 124 employee email accounts hosted on their software platform and then used that access to send a series of phishing emails to other employees. The unauthorized access led to the exposure of personal information of consumers and employees, including hundreds of New York residents who had their names, addresses, passport numbers, and driver’s license numbers exposed.

At the time of this first incident, the company had not yet implemented multi-factor authentication on its software platform, even though this was a requirement of the Regulation.

Additionally, though Carnival became aware of the incident in May 2019, they did not report it to NYDFS until April 2020 – despite the requirement that cyber incidents be reported to the agency within 72 hours. The NYDFS Order noted that this was due to the fact that Carnival’s incident response plan did not include reference to the Regulation’s notification requirement.

Carnival experienced three additional cyber incidents from August 2020 to March 2021 that followed a similar pattern: a threat actor gained unauthorized access to

¹ One area of focus for NYDFS is vulnerability to ransomware attacks. Last year, NYDFS released Ransomware Guidance highlighting specific cybersecurity controls that companies should implement.

Carnival's IT system, usually as the result of a phishing scheme, leading to the exposure of consumer personal information, including sensitive data like social security numbers and private health data.

Because Carnival is considered a Covered Entity, NYDFS expects it to meet the standards set by the Regulation. This includes implementation of MFA and cybersecurity awareness training for all personnel, which NYDFS concluded was inadequate due to the occurrence of four cyber incidents within four years – at least some of which resulted from phishing attacks. The Order also pointed out that Carnival's CISO had certified compliance with the Regulation for 2018, 2019, and 2020 – certifications that were improper given the cyber events and the underlying noncompliance that caused them.

Due to the violations identified in the Order, Carnival agreed to a \$5 million penalty. Notably, this penalty was four times higher than the \$1.25 million combined settlement Carnival reached the previous day with 45 states for failure to timely notify victims of the breach. Carnival also agreed to surrender its insurance licenses issued by NYDFS and cease selling insurance in New York. The Order marks the fourth time NYDFS has used the Regulation to fine a corporation for inadequate cybersecurity programs.

CONCLUSION & TAKEAWAYS

NYDFS's Cybersecurity Regulation can create substantial obligations to safeguard systems and report data breaches for licensees, even when the licensee's core business is not related to the financial services industry. Businesses that NYDFS supervises for even a small portion of their business should take care to implement and maintain cybersecurity practices that satisfy the Regulation, including MFA, employee training to avoid phishing attacks, and an incident response plan that incorporates the requirement to alert NYDFS within 72 hours of discovering a breach. Failure to comply with the Regulation can result in costly fines and the inability to continue conducting financial activities regulated by the NYDFS.