AN A.S. PRATT PUBLICATION
SEPTEMBER 2020
VOL. 6 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: PRIVACY AND COVID-19
Victoria Prussen Spears

CONGRESS INTRODUCES TWO PRIVACY BILLS TO REGULATE COVID-19 RELATED DATA
J.C. Boggs, Phyllis B. Sumner, Scott Ferber, and Michael Dohmann

BEYOND BORDERS: COVID-19 HIGHLIGHTS THE POTENTIAL WIDESPREAD IMPACT OF THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT
P. Russell Perdew, Taylor Levesque, and Brandan Montminy

CONTACT-TRACING APPS: A DELICATE BALANCING ACT OF WORKPLACE SAFETY AND PRIVACY RIGHTS
Scott Ferber, Michael W. Johnston, Phyllis B. Sumner, Benjamin K. Jordan, and Bailey J. Langner

THE RIGHT TO BE FORGOTTEN IN THE UNITED STATES – PART II
C. W. Von Bergen, Martin S. Bressler, and Cody Bogard

THE SEC'S CYBERSECURITY ENFORCEMENT APPROACH: WHAT FINANCIAL FIRMS NEED TO KNOW
Elizabeth P. Gray and Nicholas Chanin

PRIVACY TRIAGE: FIVE TIPS TO IDENTIFY KEY PRIVACY RISKS OF NEW PRODUCTS AND SERVICES
Alexander B. Reynolds

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 7** **SEPTEMBER 2020**

Editor's Note: Privacy and COVID-19
Victoria Prussen Spears 201

Congress Introduces Two Privacy Bills to Regulate COVID-19 Related Data
J.C. Boggs, Phyllis B. Sumner, Scott Ferber, and Michael Dohmann 203

Beyond Borders: COVID-19 Highlights the Potential Widespread Impact of the Illinois Biometric Information Privacy Act
P. Russell Perdew, Taylor Levesque, and Brandan Montminy 208

Contact-Tracing Apps: A Delicate Balancing Act of Workplace Safety and Privacy Rights
Scott Ferber, Michael W. Johnston, Phyllis B. Sumner, Benjamin K. Jordan, and Bailey J. Langner 211

The Right to Be Forgotten in the United States – Part II
C. W. Von Bergen, Martin S. Bressler, and Cody Bogard 215

The SEC's Cybersecurity Enforcement Approach: What Financial Firms Need to Know
Elizabeth P. Gray and Nicholas Chanin 223

Privacy Triage: Five Tips to Identify Key Privacy Risks of New Products and Services
Alexander B. Reynolds 227

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
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)

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

(2020–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, 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.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The SEC's Cybersecurity Enforcement Approach: What Financial Firms Need to Know

By Elizabeth P. Gray and Nicholas Chanin*

Financial firms are now operating in a world where cybersecurity events occur with increased frequency and effectiveness, and where inadequate preparation for, or response to such events will be met with regulatory scrutiny. This article discusses the Securities and Exchange Commission's enforcement approach to cybersecurity for financial firms.

The global economy, including most financial firms, have transitioned their operations from time-tested and relatively secure offices, to a new work-from-home environment. Hackers and other cyber criminals see this current crisis as an opportunity to exploit and have taken advantage of peoples' fear to push new, effective phishing campaigns, and are actively targeting security vulnerabilities inherent in our newly distributed work environment. Similarly, the regulations that govern financial cybersecurity and data breach disclosure are still fully in effect, and the regulators tasked with enforcing those rules are still actively policing their sphere. Financial firms are thus now operating in a world where cybersecurity events occur with increased frequency and effectiveness, and where inadequate preparation for, or response to such events will be met with regulatory scrutiny.

The seriousness with which the Securities and Exchange Commission ("SEC" or "the Commission") approaches cybersecurity, and with which it will enforce financial firms' cybersecurity obligations, was articulated at the recent Incident Response Forum by Kristina Littman, the Chief of the SEC's Division of Enforcement's Cyber Unit. The primary takeaway from Ms. Littman's comments, for any financial firm, is that the SEC is laser-focused on ensuring the market is appropriately protected from cybersecurity risks, and that firms that fail to meet their obligations should expect to answer to the Commission.

The SEC's focus in this area falls largely into three categories.

First, the adequacy of the controls and cybersecurity processes a firm has in place. Second, whether firms appropriately disclose cybersecurity risks and breaches. Third, trading that stems from hacks of material, non-public information.

---

* Elizabeth P. Gray is a partner in the Litigation Department and co-chair of the Securities Enforcement Practice Group at Willkie Farr & Gallagher LLP. Nicholas Chanin is an associate in the firm's Communications & Media Department and a member of the firm's Privacy and Cybersecurity Practice Group. Resident in the firm's office in Washington, D.C., the authors may be reached at egray@willkie.com and nchanin@willkie.com, respectively.

Financial firms need to take steps, before an issue arises, to ensure that, should the SEC investigate, their cybersecurity houses are in order.

CYBERSECURITY PROGRAMS

Under Regulation S-P ("Reg S-P"), all broker dealers, investment advisers, and investment companies registered with the SEC "must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[1] While these "policies and procedures" are required, Ms. Littman emphasized that the SEC does not require or expect perfection; that is, even where investigating a breach, the SEC will not typically second guess good faith judgment as to what constitutes a reasonable security program for a given business. Indeed, Reg S-P only requires the "written policies and procedures [to] be reasonably designed."[2]

While the SEC may not be in the business of second-guessing reasonable cybersecurity controls, it is still incumbent upon financial firms to determine what form those controls will take. At the end of January, 2020, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a release describing its observations of industry practices, as well a detailed framework against which firms can evaluate their own cybersecurity program.[3] Though Ms. Littman stressed during the Incident Response Forum that following OCIE's recommendations is not mandatory, it would likely behoove most financial firms to, at least, assess their program against the industry standard practices detailed by OCIE. Should the SEC investigate following an incident, which Ms. Littman stressed was more likely where there is evidence of a threat to market health, controls mapped against peer institutions and informed by the SEC's own framework will go a long way to demonstrating a program's reasonableness.

DISCLOSURES

As reasonably designed as a system of controls may be, the SEC will still expect those controls to function appropriately in the face of a security incident. One of the primary indicators of properly functioning controls, and the one most immediately evident to the SEC, is a firm's disclosure surrounding an incident, as required by Regulation S-K.[4] The SEC, according to Ms. Littman, expects firms to disclose any relevant, material cybersecurity risks or incidents, and expects those disclosures to be timely and accurate. Whether such reporting is possible will depend in large part on whether a company

---

[1] 17 C.F.R. § 248.30(a).

[2] *Id*.

[3] *See*, OCIE Cybersecurity and Resiliency Observation, *available at* https://www.sec.gov/files/OCIE Cybersecurity and Resiliency Observations.pdf.

[4] *See*, 17 C.F.R. § 229.503(c).

has clear guidelines in place to escalate information internally and provide senior management and boards the tools they need to discharge their disclosure duties.

As with the controls a firm has in place, the SEC's enforcement seeks to strike a balance between second-guessing good faith judgment and ensuring the health of the markets. One illustrative example Ms. Littman mentioned during the Incident Response Forum, was the 2018 settlement the SEC secured with Altaba, Inc. (formerly known as Yahoo!, Inc.) for $35 million. In that instance, though the company had detected the breach of what the company called its "crown jewels" (user names, passwords, etc.) within a few days in 2014, the incident was not disclosed until 2016 when the company was in the process of being purchased by Verizon, Inc, despite Yahoo! making multiple quarterly and annual filings over the course of that same period. According to the SEC, this response was "so lacking" that it amounted to misleading investors and warranted enforcement.[5] Ultimately, the Yahoo! case illustrates the importance of timeliness in disclosing incidents, which is only possible with appropriate controls that enable responsive internal communications.

Though deciding whether or not to disclose can itself be a balancing act, it is likely better, from an enforcement-risk standpoint, to err on the side of disclosure. Financial firms need to keep in mind, as they evaluate their disclosure obligations, that the SEC maintains a whistleblower program. Ms. Littman stressed that in cases where disclosure is warranted, it is in the interest of firms to be the party revealing a cyber risk to the SEC, rather than the Commission hearing from a third party. The SEC will often give financial firms the benefit of the doubt when it comes to disclosures, but firms need to ensure their controls enable truthful, fulsome, and timely reporting when required.

HACKS AND MARKET MANIPULATION

Perhaps the most straightforward area of focus for the SEC in terms of cybersecurity enforcement is where hacking is being used for market manipulation. These incidents can take multiple forms. For instance, this could occur where hackers steal information, as with the 2016 attack on the EDGAR filing system.[6] This could also take the form of attacks that take over accounts run by financial firms to execute public trading, or market manipulation via fake EDGAR filings or even fraudulent tweets. During the Incident Response Forum, Ms. Littman emphasized that, where there is evidence of a malicious actor or harm to the investing public, the SEC is more likely to investigate.

Accordingly, where hackers are trading on stolen information or otherwise manipulating the market, the firms victimized by those hackers should expect to have the Commission

[5] Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, *available at* https://www.sec.gov/news/press-release/2018-71.

[6] *See*, Foreign National and American Trader Settle Fraud Charges in EDGAR Hacking Case, *available at* https://www.sec.gov/news/press-release/2020-85.

rummaging through their cybersecurity controls. A strong cybersecurity program, and upfront disclosures, should go a long way to protecting broker dealers, public companies, or other SEC-regulated entities from becoming victims of SEC enforcement actions, as well as cyber-criminals.