AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2019
VOL. 5 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 9 NOVEMBER-DECEMBER 2019

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 [275] (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

(2019–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 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, 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.

Cybersecurity Starts at the Top: Risks and Concerns for Directors and Officers

By Matthew D. Dunn and Melissa J. Erwin*

The authors explain that the costs associated with data breaches can be significant, and that data breaches may lead to investigations by state or federal agencies, regulatory fines and sanctions, private litigation, shareholder suits, and even liability for officers and director.

While many are no doubt tired of hearing about cybersecurity, hackers and cybercriminals continue to employ sophisticated and evolving strategies to access data and disrupt organizations, and, unfortunately, this issue is not going away. Cybersecurity, however, is not only a problem for legal, compliance, and IT personnel. While many executives and boardrooms have been proactive in embracing cybersecurity best practices, for many this remains an area for improvement. Recent developments in data breach litigation cases have demonstrated that officers and directors may increasingly be in the cross-hairs of claims arising from data breaches and may be exposed to individual liability. In addition, regulatory guidance has increasingly emphasized that formation and oversight of cybersecurity programs and policies should start at the top—with executives and boards of directors.

Several key best practices for officers and directors can be distilled from the recent cases and regulatory developments. These are set forth below followed by a summary of the cases and regulatory guidance.

BEST PRACTICES FOR OFFICERS AND DIRECTORS

The following are best practices and steps that officers and directors should take to minimize cybersecurity-related risks for their organization:

- Understand the applicable laws, regulations, and guidance relating to data protection and cybersecurity, by consulting with legal advisors or otherwise. Executives and boards should have general knowledge of these matters and access to experts within or outside the organization.
- Ensure that an organizational risk assessment has been conducted and is periodically updated. Identify and address the company's specific cyber and data

* Matthew D. Dunn is a partner at Carter Ledyard & Milburn LLP, representing clients in complex litigation and cybersecurity and data privacy matters. Melissa J. Erwin is counsel at the firm, representing clients in white-collar criminal defense and commercial litigation, as well as cybersecurity and data privacy matters. The authors can be reached at mdunn@clm.com and erwin@clm.com, respectively.

protection risks in an effort to avoid the consequences and costs associated with a data breach. Officers and directors should know what types of data the organization has and how it is protected.

- Ensure that the organization has robust cybersecurity and data protection and privacy policies tailored to the organization's specific risk profile, and they are implemented and followed. Officers and directors should be familiar with these policies. Management should educate board members on cybersecurity policies and guidelines that demonstrate reasonable information security procedures and implementation of data protection standards.
- Build compliance into the governance structure. Consider whether the board should have a committee that oversees cybersecurity and data protection issues. Consider appointing a chief information security officer. Ensure that the organization has personnel charged with implementing and enforcing cybersecurity policies and procedures.
- Review the technology infrastructure for data security and information management and ensure that it is current and updated regularly (anti-virus and anti-malware software, encryption, etc.). Obtain a report from the chief information officer or IT director. Consider requiring cybersecurity updates as part of the agenda at board meetings.
- Ensure that the organization has an adequate cyber incident response plan, and that it is updated and practiced. Organizations should conduct cyber breach exercises and penetration tests.
- For public companies, ensure that there are effective disclosure controls and procedures that enable the organization to make accurate and disclosures relating to cybersecurity. Ensure that public filings adequately address cybersecurity risks, policies, oversight, and incidents.
- Ensure that there is employee training and education on cyber and data protection policies, and the identification of red flags.
- Conduct risk assessment of third-party vendors. Ensure that vendors with access to the organization's data have adequate cybersecurity and privacy policies to protect such data.
- Review and assess insurance coverage for data breaches and cyber-related incidents, and consider separate cybersecurity insurance. Review and assess whether directors and officers insurance covers cybersecurity-related liability.

DATA BREACH CASES: CLAIMS AGAINST DIRECTORS AND OFFICERS

Officers and boards of directors owe two primary fiduciary duties to their organization—the duty of care and the duty of loyalty. The duty of care requires directors and officers to exercise the level of care that a prudent person would use under similar circumstances, which includes not consciously disregarding red flags when there is a duty to take action. There is generally no liability for decisions reasonably made by officers and directors in good faith. The duty of loyalty requires directors and officers to refrain from benefiting themselves at the expense of the corporation that they serve and to refrain from conduct that injures the corporation. In the seminal case on the subject, *In re Caremark International*, the Delaware Chancery Court stated that a director's duty of care "includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."[1]

In the early data breach cases, claims against officers and directors were typically dismissed during motion stages. For example, in, *Palkon v. Holmes*, a New Jersey federal court dismissed a shareholder derivative suit against Wyndham Worldwide Corporation and its officers and directors arising out of three data breaches between 2008 and 2010 that resulted in hackers obtaining personal and financial data of over 600,000 customers, holding that the board's actions were a proper exercise of its business judgment because the board had acted reasonably and had addressed cybersecurity concerns numerous times.[2] In another case, *In re Home Depot Shareholder Derivative Litigation*, a Georgia federal court dismissed a case brought by shareholders in response to a 2014 data breach that resulted in the theft of personal financial data of 56 million Home Depot customers, holding that plaintiffs failed to set forth facts showing that the board "consciously failed to act in the face of a known duty to act," and that "[d]irectors' decisions must be reasonable, not perfect."[3]

Earlier this year, a court-approved settlement in *In re Yahoo! Shareholder Litigation*,[4] has shaken the sense of security (no pun intended) officers and directors may have been feeling after earlier data breach decisions. In January 2019, a California state court approved a $29 million settlement of three shareholder derivative suits against Yahoo and former officers and directors, including the former CEO, which was the first instance of monetary recovery in a data breach shareholder derivative suit that targeted officers and directors for breach of fiduciary duty.

---

[1] 698 A.2d 959, 970 (Del. Ch. 1996).
[2] No. 2:14-CV-01234, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014).
[3] 223 F. Supp. 3d 1317 (N.D. Ga. Nov. 30, 2016).
[4] Case No. 17-CV-307054 (Cal. Sup. Ct., Santa Clara Co. Jan. 4, 2019).

The *Yahoo* case arose from allegations that the former officers and directors breached their fiduciary duties by engaging in a years-long plot and sham investigation to conceal multiple cyberattacks dating from 2013 to 2016. This active concealment included a 2014 cyberattack that resulted in Russian hackers stealing user information associated with at least 500 million user accounts, which was not disclosed until 2016 after Yahoo and Verizon entered into a stock purchase agreement, as well as additional breaches impacting billions of Yahoo user accounts which were also discovered to have been concealed by Yahoo's directors and officers. As a result of Yahoo's disclosure of the 2014 cyberattack in 2016, the purchase price for Yahoo was ultimately reduced by $350 million and Yahoo agreed to retain 50 percent of the liabilities associated with the data breach and 100 percent of the liabilities from shareholder lawsuits arising from the breach. In addition, as described below, in April 2018, Yahoo's successor, Altaba, agreed to a $35 million settlement with the Securities and Exchange Commission ("SEC") for its failure to timely disclose the data breach. Given the egregious allegations and the SEC settlement, Yahoo agreed to pay $29 million to settle the consolidated cases. It is likely that this case will provide a roadmap for future shareholder suits against officers and directors in the data breach context.

In the same month, in *In re Equifax Inc. Securities Litigation*, a data breach class action case against the credit-rating firm Equifax and certain officers and directors arising out of a cyberattack in which criminal hackers breached Equifax's computer network and obtained personally identifiable information of more than 148 million American Equifax customers, a Georgia federal court granted in part and denied in part a motion to dismiss.[5] The lead plaintiff, representing a class of shareholders, alleged violations of the securities laws by officers and directors who made false and misleading statements about the vulnerability of the company's computer systems to cyberattack and its compliance with data protection laws and best practices, and failed to take basic steps to protect its computer systems. The court granted the motion to dismiss with respect to the claims against most of the officers and directors; however, it denied the motion as to Equifax's former CEO and Chairman of the Equifax Board, who was alleged to have had personal knowledge that Equifax's data protection systems were "grossly inadequate" and yet knowingly or recklessly made false and misleading statements about the company's data security, and had the power to control cybersecurity policies and the statements made about such policies that resulted in securities law violations.[6]

Courts will likely be less understanding over time as the hacks keep coming, and the business judgment rule will not protect a board that does not have its eyes on cybersecurity.

[5] 357 F. Supp. 3d 1189 (N.D. Ga. Jan. 28, 2019).
[6] *Id.* at 1240-52.

SEC AND OTHER REGULATORY GUIDANCE AND ENFORCEMENT

While the SEC has for years warned companies about cybersecurity risks and related reporting obligations, in 2018 it issued new interpretative guidance concerning the obligations of publicly traded companies to disclose cybersecurity incidents and issues.[7] In October 2018, the SEC issued an investigative report which emphasized that issuers, in complying with the requirement to have sufficient internal accounting controls, should consider cyber-related threats, including protection against spoofed or manipulated electronic communications.[8]

The SEC has specifically emphasized that it is the board's role to understand the risks, ensure that the company is addressing those risks, and oversee the company's cybersecurity program. The SEC indicates that companies should, as part of their proxy statement, disclose the board's involvement in cybersecurity efforts and risk management, and should specifically indicate "the nature of the Board's role in overseeing the management of that risk."[9] SEC Commissioner Robert J. Jackson, Jr., in a 2018 speech relating to cybersecurity, reinforced the important role and obligations of officers and directors:

> In short: the cyber threat is a corporate governance issue. The companies that handle it best will have relevant expertise in the boardroom and the C-suite, a strategy for engagement with investors and the public, and—most of all—sound advice from corporate counsel who can navigate uncertain times and uncertain law in a critical area for the company's business.[10]

---

[7] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Securities and Exchange Commission (Feb. 21, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf. The SEC has made clear that it expects companies to have comprehensive cybersecurity policies and procedures, to be transparent regarding cyber risks, security, and incident preparedness, and to make timely and non-generic disclosures in public filings. The SEC expects companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, and reputational consequences." Further, the SEC requires companies to "establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."

[8] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Exchange Act Release No. 84429 (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

[9] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR Parts 229 and 249, SEC Release Nos. 33-10459 and 34-82746 (Feb. 6, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[10] Robert J. Jackson Jr., Commissioner, Securities and Exchange Commission, Corporate Governance: On the Front Lines of America's Cyber War (Mar. 15, 2018), https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15.

Although this 2018 guidance related only to public companies, the SEC has issued guidance and best practices for other regulated entities under the federal securities laws, such as investment advisers, broker-dealers, and self-regulatory organizations, and has a website dedicated to cybersecurity issues, which similarly focus on the importance of well-implemented cybersecurity policies and procedures.[11]

The SEC has begun bringing enforcement actions in connection with cybersecurity-related failures and misconduct, and such enforcement actions will likely increase in the coming years. In March 2018, the SEC filed an enforcement action (with parallel criminal charges) against the former Chief Information Officer of a U.S. business unit of Equifax for insider trading in connection with the sale of shares prior to the public disclosure of a massive data breach.[12] As a result of the SEC enforcement action, the executive was ordered to pay disgorgement and prejudgment interest totaling $125,636 and is prohibited from acting as an officer or director of any public company for a period of ten years, and was also sentenced to four months in federal prison in the parallel criminal action.[13] In April 2018, the SEC imposed a $35 million penalty on Yahoo successor Altaba, in the SEC's first cybersecurity enforcement action against a public company for failing to timely disclose a data breach.[14] In September 2018, a broker-dealer and investment adviser agreed to pay $1 million to settle SEC charges related to its failure to have sufficient cybersecurity policies and procedures to prevent a cyber intrusion that compromised personal information of thousands of

[11] *See* Spotlight on Cybersecurity, the SEC, and You, https://www.sec.gov/spotlight/cybersecurity; *see also* Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies, SEC Risk Alert (Apr. 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf (risk alert for investment advisers and broker-dealers, which emphasized that Regulation S-P requires registrants to have written policies and procedures for the protection of customer records and information); Cybersecurity Guidance, SEC Division of Investment Management (Apr. 2015), https://www.sec.gov/investment/im-guidance-2015-02.pdf (cybersecurity guidance for registered investment companies and registered investment advisers); Observations from Cybersecurity Examinations, SEC Risk Alert (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf (observations and guidance from cybersecurity examinations of broker-dealers, investment advisers and investment companies); SEC Staff Guidance on Current SCI Industry Standards (Nov. 19, 2014), https://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf (adoption of Regulation Systems Compliance and Integrity applicable to certain self-regulatory organizations, including registered clearing agencies, alternative trading systems, plan processors, and exempt clearing agencies).

[12] Former Equifax Executive Charged With Insider Trading, SEC Press Release No. 2018-40 (Mar. 14, 2018), https://www.sec.gov/news/press-release/2018-40.

[13] SEC Obtains Final Judgment Against Former Equifax Executive Charged with Insider Trading, SEC Litigation Release No. 24541 (July 18, 2019), https://www.sec.gov/litigation/litreleases/2019/lr24541.htm; Former Equifax employee sentenced for insider trading, U.S. Department of Justice (June 27, 2019), https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading.

[14] Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, SEC Press Release No. 2018-71 (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

customers, which was the first of its kind enforcement action for violations of the Safeguards Rule and the Identity Theft Red Flags Rule, which are designed to protect confidential customer information and protect customers from the risk of identity theft.[15]

Companies may also be subject to state cybersecurity and data breach laws, such as the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies, which imposes various requirements on banks, insurance companies, and other covered entities, and the newly enacted Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act") which amends and broadens New York's data breach notification law applicable to those who own or license private information of New York residents. Companies may be subject to data protection laws, including the European Union's General Data Protection Regulation ("GDPR"). In addition, the Federal Trade Commission, Department of Health and Human Services, and Federal Communications Commission regulate data privacy and security in specific contexts.

CONCLUSION

Given the continued threat of cyberattacks and breaches, strong corporate defenses and best practices should start at the top—with officers and directors. The costs associated with data breaches can be significant, and data breaches may lead to investigations by state or federal agencies, regulatory fines and sanctions, private litigation, shareholder suits, and even liability for officers and directors. Executives and boards are encouraged to consult counsel regarding cybersecurity compliance and initiatives.

[15] SEC Charges Firm With Deficient Cybersecurity Procedures, SEC Press Release No. 2018-213 (Sept. 26, 2018), https://www.sec.gov/news/press-release/2018-213.