AN A.S. PRATT PUBLICATION
MAY 2018
VOL. 4 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 NUMBER 4 MAY 2018

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*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [107] (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

(2018–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, 718.224.2258. 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 Show and Tell: SEC Guidance on Cybersecurity Disclosures

By Alaap B. Shah and Robert J. Hudock*

The authors of this article explain the recently issued interpretive guidance on cybersecurity related disclosures and controls issued by the U.S. Securities and Exchange Commission, which discusses obligations under current laws and regulations and the need for robust cybersecurity policies and procedures governing disclosures and prohibiting insider trading.

The U.S. Securities and Exchange Commission ("SEC") recently issued interpretive guidance[1] on cybersecurity related disclosures and controls. This guidance reaffirms, and expands upon, prior staff guidance[2] from 2011 as well. This guidance also adds emphasis to the prior staff guidance by constituting a statement of the Commission. Collectively these documents provide guidance to publicly-traded companies about how to factor cybersecurity risk and cybersecurity incidents into policy development and decision-making related to public disclosure, prohibition on insider trading and selective disclosure under Regulation FD. Specifically, this interpretive guidance discusses obligations under current laws and regulations and the need for robust cybersecurity policies and procedures governing disclosures and prohibiting insider trading.

GROWING CYBERSECURITY RISK

Through the recent interpretive guidance, the SEC trumpeted growing cybersecurity risks impacting the capital markets. In particular, the SEC provided warning regarding cybersecurity incidents by stating "The objectives of cyber-attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners." Recognizing these risks, the SEC describes the impact cybersecurity incidents can have on public companies including the following:

---

* Alaap B. Shah is a member of the firm in the Health Care and Life Sciences practice at Epstein Becker & Green, P.C., advising clients on federal and state privacy and data security laws and regulations, cybersecurity and data breach matters, and health care fraud and abuse issues. Robert J. Hudock, a member of the firm in the Health Care and Life Sciences group, focuses his practice on data breach and response, national security law, cybersecurity, and global privacy and data security. Resident in the firm's Washington, D.C., office, the authors may be contacted at abshah@ebglaw.com and rhudock@ebglaw.com, respectively.

[1] https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[2] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

- "remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack [including ransom];
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;
- increased insurance premiums;
- reputational damage that adversely affects customer or investor confidence; and
- damage to the company's competitiveness, stock price, and long-term shareholder value."

As a result of this heighted awareness of the impacts of cybersecurity issues and the importance of transparency to investors related to company management of such issues, the SEC's guidance on what is required of publicly-traded companies in this climate comes at a critical time.

MATERIALITY OF CYBERSECURITY INFORMATION

The recent interpretive guidance makes clear that the SEC sees cybersecurity information as a significant factor that investors weigh when making decisions about trading any given publicly-traded company's securities. The SEC continues to apply its "materiality" when determining whether a public company is required to disclose cybersecurity related information to the public. Nevertheless, the interpretive guidance reinforces that cyber security information is currently among one of the most significant factors that make investment in the public company's securities speculative or risky. As such, public companies should take a hard look at the non-public information in its possession to determine whether disclosure would be required under current laws and regulations.

DISCLOSURE REQUIREMENTS

The recent interpretive guidance reaffirms prior guidance stating that disclosure regarding cybersecurity risks and incidents is required when the information is "material" such that "there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available." The guidance further establishes that "materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations."

When a public company determines cybersecurity information is material, it must disclose such information in a timely manner. The SEC guidance establishes that disclosures should be tailored to the public company and the cybersecurity risks it faces. Further, the guidance reaffirms, but also expands on the 2011 guidance regarding the kinds of information that should be considered for disclosure. These can include, but are not limited to, information related to cybersecurity risk factors, cybersecurity incidents, operational issues related to cybersecurity management or the impact of litigation or government investigations.

Disclosure of Risk Factors

The SEC largely continues to rely on the probability/magnitude test.[3] Applying the principles related to probability of occurrence and magnitude of harm, the SEC provided guidance related to what material information companies should consider disclosing. These include, but are not limited to, the following:

- Probability of cyber-incidents occurring;
- Quantitative and qualitative magnitude of cybersecurity related risks;
- Adequacy of measures to prevent cybersecurity incidents from occurring (and limitations on the public company to prevent incidents);
- The context of risk relative to prior cybersecurity incidents and severity and frequency of those incidents;
- A description of the public company's business/operations that give rise to material cybersecurity risk;
- Outsourced functions posing cybersecurity risks and how the public company addresses such risks;
- Industry-specific cybersecurity risks;
- Risks related to cybersecurity incidents that may go undetected;
- Relevant insurance coverage to offset losses resulting from cybersecurity incidents; and
- Potential harm/costs/consequences related to cybersecurity incidents.

When evaluating potential harm, cost and consequences related to a cybersecurity issue, the following factors should be considered:

- Reputation;
- Financial performance;

[3] *See Basic v. Levinson,* 485 U.S. 224 (1988).

- Customer relationships;
- Vendor relationships;
- Litigation;
- Regulatory investigations; and
- Existing or pending laws or regulations that may affect the public company related to cybersecurity and associated costs.

Public companies may want to consider disclosing other factors it finds to be materials to allow investors to make informed investment decisions.

Disclosure of Cybersecurity Incidents, Litigation, and Company Cybersecurity Posture

Further, the recent guidance reiterates that disclosure should not be limited just to risk factors, but also should provide investors insight into material information related to actual occurrences and a public company's cybersecurity posture. First, a publicly-traded company should consider disclosing material information related to cybersecurity incidents that have occurred along with related costs, consequences and mitigation efforts. Second, a public company should consider disclosing material information related to the extent of its Board's role in oversight and administration or delegation of this oversight function. Third, to the extent a company is involved in litigation related to a cybersecurity issue, disclosures should include the following:

- name of court;
- date of proceedings;
- principal parties;
- factual bases alleged; and
- relief sought.

Timeliness of Disclosure, Scope, Delay, and Subsequent Amendment

The interpretive guidance reaffirms the need for a company to make accurate and timely disclosures of material events related to cybersecurity. Yet, the SEC guidance reaffirmed that certain circumstances may allow for delay of disclosure such as a company's legitimate need to investigate further or cooperate with law enforcement. Nevertheless, the SEC guidance qualifies that, if information related to an incident is material, policies and procedures should require a public company to make timely disclosures which can be subsequently augmented or corrected as more information is obtained. In addition, while recent guidance points to a wide variety of information that could be considered materials and warrant disclosure, the SEC makes clear that there is no requirement to disclose information that would compromise the cybersecurity of the public company.

PROHIBITION ON INSIDER TRADING AND SELECTIVE DISCLOSURES UNDER REGULATION FD

The interpretive guidance reaffirms that the anti-fraud provisions relating to insider trading prohibition are triggered when trading on material, non-public information related to cybersecurity risks and incidents. Particularly, the SEC views trading by corporate insiders having knowledge of material information after the occurrence of a cybersecurity incident, but prior to public disclosure, to raise the appearance of insider trading in violation of SEC's anti-fraud rules. Likewise, trading after only selective disclosures of material cybersecurity information have been made under Regulation FD would also raise the appearance of insider trading. To prevent such issues, the SEC encourages public companies to consider how and when to implement blackout periods where trading would be restricted for corporate insiders.

CONTROL AND PROCEDURE IMPLEMENTATION

To operationalize compliance with the recent interpretive guidance, the SEC encourages public companies to revisit their policies and procedures to evaluate the adequacy of control procedures. Specifically, public companies should consider implementing policies and procedures to accomplish the following:

- Determine materiality of cybersecurity-related risks and incidents;
- Ensure public company directors, officers, and other key stakeholders who are responsible for development and oversight of cybersecurity programs are informed so the public company can make timely disclosure decisions and certifications regarding cybersecurity issues;
- Prohibit and prophylactically prevent corporate insiders from trading on public company securities while in possession of material, non-public information related to cybersecurity issues (this could be accomplished through a code of ethics, code of conduct or other policies);
- Ensure timely public disclosure of material cybersecurity issues through period reports, registration statements, current reports, and other filings;
- Ensure public disclosures are not selective in terms of content or audience (i.e. even if selective disclosures are permitted under Regulation FD); and
- Ensure that partial or inaccurate disclosures are augmented/amended/corrected when new information is available to the public company.

Public companies should also routinely evaluate the adequacy of policies and procedures on an on-going basis to facilitate compliance with disclosure requirements and prohibitions on insider trading related to cybersecurity issues.

BUILDING A CULTURE OF COMPLIANCE

As the frequency and impact of cybersecurity incidents increases over time, the SEC makes clear that it considers certain cybersecurity information to be material as it is included among the most significant factors that make investment in the public company's securities speculative or risky. As such, the SEC emphasizes through this guidance that public companies should endeavor to disclose material, non-public information in a timely manner.

In order to comply with this general requirement, the SEC encourages public companies to revisit their disclosure policies and procedures to ensure adequate controls are in place to facilitate appropriate disclosure of cybersecurity-related information to the public. Public companies that have yet to implement such policies and procedures should work immediately to implement comprehensive cybersecurity disclosure policies, procedures and other operational controls. Public companies that have implemented cybersecurity disclosure policies and procedures are still encouraged to revisit those policies and procedures and make updates as needed.

Similarly, publicly-traded companies should have a keen focus on implementing robust policies and procedures to prohibit and prophylactically prevent insider trading based on material, non-public cybersecurity information. These efforts should include policies that reduce risk related to trading on information that has only selectively been shared under Regulation FD.

Finally, beyond developing adequate controls, the SEC also stresses that publicly-traded companies address the adequacy of governance and operational structures to promote awareness and oversight regarding cybersecurity issues from the Board level down through an organization.