AN A.S. PRATT PUBLICATION
OCTOBER 2023
VOL. 9 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 NUMBER 8 October 2023

LexisNexis®

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
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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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 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.

Securities and Exchange Commission Adopts New Rules on Cybersecurity Incident Reporting and Disclosure for Public Companies

By Adam Aderton, Daniel K. Alvarez, Elizabeth P. Gray, Laura E. Jehl, A. Kristina Littman, Nicholas Chanin, Erik Holmvik and Marc J. Lederer*

In this article, the authors discuss the new cybersecurity rules adopted by the Securities and Exchange Commission that make it imperative that all registrants have mature cybersecurity risk management processes, well integrated with company leadership.

The Securities and Exchange Commission (the SEC or Commission) has voted 3-2[1] to adopt new rules (New Rules) to enhance and standardize timely disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (the Exchange Act).[2] The New Rules have added a new Item 1.05 on Form 8-K where registrants must disclose a material cybersecurity incident within four days of management's determination that the incident is material, subject only to a narrow exception for national security issues. The New Rules also include updated cybersecurity risk management, strategy, and governance disclosure obligations in Forms 10-K and 10-Q, including disclosures regarding management's role in assessing and managing risks from cybersecurity threats.

I. BACKGROUND

The New Rules, originally proposed in March 2022,[3] are the SEC's first formally adopted rules addressing cybersecurity practices and disclosures of cybersecurity incidents for public companies. The New Rules build on previous SEC interpretive

* The authors, attorneys with Willkie Farr & Gallagher LLP, may be contacted at aaderton@willkie.com, dalvarez@willkie.com, egray@willkie.com, ljehl@willkie.com, aklittman@willkie.com, nchanin@willkie.com, eholmvik@willkie.com and mlederer@willkie.com, respectively.

[1] For a discussion of Commissioners Hester Peirce and Mark Uyeda's dissenting statements, See Infra Section III(C).

[2] U.S. Securities and Exchange Commission, Final Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release Nos. 33-11216; 34-97989; File No. S7-09-22 (Jul. 26, 2023), https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

[3] See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (Mar. 9, 2022), https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf.

guidance regarding cybersecurity disclosures from 2011[4] and 2018,[5] as well as Regulation SCI's specific requirements for Self-Regulating Organizations and Clearing Agencies.[6] While the SEC's previously-issued guidance provided registrants with some insight regarding information that the SEC deemed material, no previously existing disclosure requirement explicitly referred to cybersecurity risks and cyber incidents.

Additionally, the SEC found that current cybersecurity disclosure practices [are] too varied, making it difficult for investors to locate, interpret, and analyze the information registrants provided.[7]

One of the SEC's primary stated motivations for the New Rules is its belief that investors would benefit from more timely and consistent cybersecurity disclosures to make informed investment decisions. A statement released by Chair Gary Gensler on the same day that the New Rules were adopted explained his belief that under the New Rules, cybersecurity disclosures will be "more consistent, comparable and decision-useful."[8]

II. CYBERSECURITY INCIDENT REPORTING REQUIREMENT

A. Four-Day Incident Reporting

The most notable aspect of the New Rules is a requirement that registrants disclose a material cybersecurity incident[9] within four days of management's determination, without unreasonable delay in making that determination, that the incident is material.[10] Registrants will make these disclosures on the new Item 1.05 of Form 8-K, and should include in their disclosure all known material aspects of the incident, including: (1) the nature, scope, and timing of the incident, and (2) the incident's impact or

[4] U.S. Securities and Exchange Commission, Division of Corporate Finance Disclosure Guidance: Topic No. 2 Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[5] U.S. Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release Nos. 33-10459; 34-82746 (Feb. 26, 2018), https://www.sec.gov/files/rules/interp/2018/33-10459.pdf.

[6] See SEC Regulation Systems Compliance and Integrity, 17 C.F.R. §§ 240, 242, and 249 (2014), https://www.govinfo.gov/content/pkg/FR-2014-12-05/pdf/2014-27767.pdf.

[7] Supra note 2 at pp. 6-7.

[8] Press Release, U.S. Securities and Exchange Commission, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Jul. 26, 2023), https://www.sec.gov/news/press-release/2023-139.

[9] Cybersecurity Incident" as defined by the adopted New Rules means: "An unauthorized occurrence, or series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." Supra note 2, at p. 76.

[10] Supra note 2 at p. 37.

reasonably likely impact on the registrant, including its financial condition and results of operations.[11]

The Commission also clarified that a series of individually immaterial events, which become material in the aggregate, may trigger Item 1.05 reporting requirements,[12] as might incidents that occur on a third-party service provider's systems.[13] Additionally, the Commission added an Instruction 4 to Item 1.05 to provide that a "registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." Finally, to the extent information regarding a material cybersecurity incident is unavailable or not determined at the time of filing the initial Form 8-K, registrants are directed to identify these gaps on their initial Form 8-K and to subsequently update their initial filing after such information becomes available.[14]

The New Rules are slightly narrower in scope than those proposed in March 2022. For example, a registrant is no longer required to disclose information regarding cybersecurity incident remediation status, and "need not disclose specific or technical information about its planned response to the incident."[15] Further, the determination of materiality, which prompts disclosure, must be made "without unreasonable delay" rather than "as soon as reasonably practicable."[16] Finally, the Commission decided not to adopt proposed Items 106(d)(1)[17] and (2),[18] which required registrants to provide updated disclosures in periodic reporting regarding incidents previously disclosed pursuant to Item 1.05 of Form 8-K.[19]

---

[11] Id. p. 29.

[12] Supra note 2 at p. 53.

[13] Id. p. 78-79.

[14] Id. pp. 50-51.

[15] Id. p. 30.

[16] Id. p. 37.

[17] As proposed, Item 106(d)(1) would have required disclosure, in periodic reports, of the following: (1) Any material effect of the incident on the registrant's operations and financial condition; (2) Any potential material future impacts on the registrant's operations and financial condition; (3) Whether the registrant has remediated or is currently remediating the incident; and (4) Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes. Supra note 2, at p. 46.

[18] As proposed, Item 106(d)(2) would have required disclosure in periodic reports when a registrant determines that a series of previously undisclosed but related immaterial cyberattacks amount to having a material effect: (1) A general description of when the incidents were discovered and whether they are ongoing; (2) A brief description of the nature and scope of the incidents; (3) Whether any data were stolen or altered in connection with the incidents; (4) The effect of the incidents on the registrant's operations; and (5) Whether the registrant has remediated or is currently remediating the incidents. Supra note 2, at p. 47.

[19] See supra Section II(A) for a discussion of the requirement to file an amended Form 8-K to incidents disclosed pursuant to Item 1.05.

B. The National Security Exception

The only exception to the four-day disclosure requirement included in the New Rules is for those instances where disclosure would present a substantial risk to national security or the public interest.[20] However, registrants may only rely on this exception with a written determination from the Attorney General to the Commission that such a substantial risk exists. Notably, this exception is only temporary; the Attorney General can delay disclosure for a period of time specified by the Attorney General, not to exceed 30 days, which, with further coordination between the Attorney General and the Commission, can be extended to 120 days.[21] Given the high standard to meet this threshold and the requirement to obtain a written determination from the Attorney General, use of this exception is likely to be extremely limited.

III. UPDATED 10-K AND 10-Q DISCLOSURE REQUIREMENTS

A. Processes Disclosures

The New Rules also amend Regulation S-K, requiring new cybersecurity disclosures on Forms 10-K and 10-Q. Registrants will now be required to describe their "processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes."[22] As with the new cybersecurity incident reporting requirements, the New Rules require registrants to make forward-looking disclosures on their periodic reports regarding whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.[23] Other disclosure requirements include:

- Whether and how the registrant's cybersecurity processes have been integrated into its overall risk management system or processes;
- Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

[20] Supra note 2 at p. 11.

[21] Supra note 2 at p. 34.

[22] Id. p. 61.

[23] Id. p. 29-30. The adopting release notes the rule's inclusion of "financial condition and results of operations" is not exclusive; companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. "Harm to a company's reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the company. Similarly, the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal governmental authorities and non-U.S. authorities, may constitute a reasonably likely material impact on the registrant."

- Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.[24]

Though the New Rules increase the disclosure burden on registrants, the New Rules were pared back from those originally proposed in March 2022. Notably, the Commission requires registrants to disclose "processes" for managing material cybersecurity risks rather than "policies and procedures" to alleviate concerns that disclosures would require registrants to divulge "the kinds of operational details that could be weaponized by threat actors."[25] Additionally, a list of enumerated, nonexclusive disclosure elements was removed in response to comments asserting that such disclosures would require excessive granularity, which would advantage threat actors, in addition to being unnecessarily prescriptive.[26]

B. Governance Disclosures

Registrants will also be required to disclose internal governance structures designed to oversee cybersecurity risk. Specifically, registrants will have to disclose a description of the board's oversight of material cybersecurity risks, and if applicable, identify any board committee or subcommittee responsible for such oversight, and describe the processes by which the board or such committee is informed about such risks.[27] Further, the New Rules direct, but do not require, registrants to consider disclosing the following as part of a description of management's role in assessing and managing material cybersecurity risks:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.[28]

[24] Id. pp. 62-63.
[25] Supra note 2 at p. 61.
[26] Id. p. 62.
[27] Id. pp. 68-69.
[28] Id. p. 70.

As with the disclosures concerning registrants' cybersecurity risk management processes, the Commission made significant modifications in the adopted New Rules to requirements regarding governance oversight of a registrant's cybersecurity risk. The requirements, implemented at Regulation S-K Item 106(c)(2), are less granular than originally proposed. The adopted New Rules removed requirements that registrants disclose the frequency of board discussions regarding cybersecurity and whether, and how, the Board integrates cybersecurity into its business strategy, risk management and financial oversight.[29] Notably, the SEC abandoned the requirement that registrants disclose the cybersecurity expertise of board members after being persuaded that cybersecurity process decisions are primarily designed and administered by management, rather than at the board level.[30]

The New Rules will also require parallel cybersecurity disclosure requirements from foreign private issuers in Forms 20-K and 6-K.[31]

C. Possible Challenges

Regardless of such efforts, the as-adopted New Rules were not without criticism. The New Rules were adopted by a 3-2 vote, with Commissioners Hester Peirce and Mark Uyeda issuing statements in dissent. Commissioner Peirce argued that the New Rules will be unnecessary and costly to companies.[32] She also expressed concern that the information may be more helpful to would-be hackers than investors. Commissioner Uyeda argued the New Rules elevated cybersecurity disclosures above those required for other risks and issues, "some of which may be more material to investors."[33] He also stated that the New Rules, specifically the new Item 1.05 disclosures, "break new ground" by requiring "real-time, forward-looking disclosure." Finally, Commissioner Uyeda stated the decision to not designate the New Rules as a "major rule" under the Small Business and Regulatory Enforcement Act was "not credible or supportable."[34] By calling attention to specific aspects of the New Rules, the dissenting Commissioners may be providing a road map for would-be challengers.

---

[29] Id. pp. 68-69.

[30] Id. pp. 83-85.

[31] Supra note 2 at p. 87.

[32] Hester M. Peirce, Commissioner, U.S. Securities & Exchange Commission, Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Jul 26, 2023), https://www.sec.gov/news/statement/peirce-statement-cybersecurity-072623.

[33] Mark T. Uyeda, Commissioner, U.S. Securities & Exchange Commission, Statement on the Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Jul. 26, 2023), https://www.sec.gov/news/statement/uyeda-statement-cybersecurity-072623.

[34] Id.

IV. KEY TAKEAWAYS AND NEXT STEPS

These New Rules make it imperative that all registrants have mature cybersecurity risk management processes, well integrated with company leadership. Not only must these processes be disclosed under the New Rules, but the four-day cybersecurity incident reporting requirement leaves little margin for error. Without strong cybersecurity risk management governance processes, including service provider and vendor oversight, it may be very difficult to comply with this narrow window. In addition, the extremely limited disclosure exception the New Rules provide indicates that the Commission expects registrants to disclose most material cybersecurity incidents. The SEC also has a proposal in the works to create new and revised cybersecurity requirements for investment funds, advisers, broker-dealers, market entities and others.[35] The Commission is taking cybersecurity seriously, and all companies regulated by the SEC should expect to be required to shore up their governance processes.

The New Rules took effect on September 5, 2023. Registrants will be required to include updated disclosures under Item 106 of Regulation S-K, primarily affecting Forms 10-K and 10-Q, beginning with annual reports for fiscal years ending on or after December 15, 2023. Larger registrants must comply with the incident disclosure requirements as of December 18, 2023, and smaller reporting companies must comply as of June 15, 2024.[36]

[35] Press Release, U.S. Securities and Exchange Commission, SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds (Feb. 9, 2022), https://www.sec.gov/news/press-release/2022-20.

[36] Supra note 2 at p. 107.