AN A.S. PRATT PUBLICATION
JUNE 2022
VOL. 8 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 NUMBER 5 June 2022

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*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [149] (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

(2022–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.

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

SEC Proposes Substantial New Cybersecurity Requirements for Investment Advisers and Companies

By Scott F. Mascianica and Shardul Desai*

The authors provide a summary of the new cybersecurity requirements in rules proposed recently by the Securities and Exchange Commission and offer some key takeaways.

Following U.S. Securities and Exchange Commission ("SEC") Chair Gary Gensler's recent speech[1] directing the agency to expand cybersecurity requirements on regulated entities, the SEC on February 9, 2022, voted to propose new cybersecurity requirements for investment advisers, investment companies and business development companies. Although certain rules concerning consumer data security and identity theft protection – such as Regulation S-P and Regulation S-ID – already exist for these entities, the SEC's latest proposal is a significant evolution toward far more proscriptive cybersecurity program requirements. The "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies" Proposed Rule[2] actually consists of a suite of rules (proposed rules) expressly requiring written cybersecurity risk assessments, the development of certain cybersecurity policies and procedures, cybersecurity incident reporting and cyber incident record-keeping.

The SEC claimed that these proposed rules will provide a number of market benefits, including:

- Promoting a more comprehensive framework to address cybersecurity risks;
- Reducing risks that adviser and funds cannot maintain operational capability when victimized by a cybersecurity incident;
- Providing investors with better information to make investment decisions; and

[*] Scott F. Mascianica, a partner in the Dallas office of Holland & Knight LLP, is a member of the firm's White Collar Defense and Investigations Team and the Securities Enforcement Defense Team. Shardul Desai, a partner in the firm's office in Washington, D.C., focuses his practice on cybersecurity, data privacy, and white collar defense and government investigations. The authors may be contacted at scott.mascianica@hklaw.com and shardul.desai@hklaw.com, respectively.

[1] https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.

[2] https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

- Giving the Commission "better information with which to conduct comprehensive monitoring and oversight of ever-evolving cybersecurity risks and incidents affecting advisers and funds."[3]

PROPOSED CYBERSECURITY REQUIREMENTS

The SEC's proposed rules would require registered investment advisers ("advisers") and investment companies ("funds") to:

- Develop, and periodically update, written cybersecurity risk assessments and to adopt and implement specific written cybersecurity policies and procedures reasonably designed to address cybersecurity risks;
- Disclose significant cybersecurity risks and cybersecurity incidents that affect advisers and funds and their clients and shareholders on Form ADV Part 2A and associated fund forms; and
- Adhere to new record-keeping requirements under the Advisers Act and Investment Company Act.

Additionally, advisers would be required to report significant cybersecurity incidents affecting the adviser or its fund or private fund clients to the Commission.

RISK ASSESSMENT AND CYBERSECURITY POLICIES AND PROCEDURES

The SEC explicitly noted that "there are no Commission rules that specifically require firms to adopt and implement comprehensive cybersecurity programs."[4] Now, under the proposed rules, advisers and funds that are registered or required to be registered will have to implement cybersecurity policies and procedures addressing a number of elements.

Generally speaking, the rules would require these entities to conduct cybersecurity risk assessments, document such assessments in writing, and develop and implement policies and procedures that address:

- User security and access (including acceptable use policies, authentication/MFA policies, password management policies and privileged access management policies);
- Information protection (including assessments related to data governance, encryption and network segmentation);

[3] *Id*. at 14-15.
[4] *Id*. at 13.

- Threat and vulnerability management; and
- Cybersecurity incident response and recovery.[5]

As part of the risk assessment and cybersecurity policies and procedures, advisers and funds are expected to "[i]dentify their service providers that receive, maintain or process adviser or fund information, or that are permitted to access their information systems, including the information residing therein, and identify the cybersecurity risks associated with such providers."[6] Thus, advisers and funds may need to consider – and document – cybersecurity due diligence reviews of third-party vendors.

The proposed rules also would require an annual review of these assessments, policies and procedures in which an adviser reviews and assesses the design and effectiveness of the cybersecurity policies and procedures and prepares a written report that, at a minimum, describes the review, assessment and control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.

Similarly, for funds, the SEC would require fund's board of directors to initially approve the fund's cybersecurity policies and procedures and to review the fund's written reports on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures. If the rules are approved, these written reports will be required at least annually.

The agency acknowledged that "there is not a one-size-fits-all approach to addressing cybersecurity risks" and "[t]he proposed cybersecurity risk management rules therefore give advisers and funds the flexibility to address the general elements based on the particular cybersecurity risks posed by each adviser's or fund's operations and business practices."[7] Yet, while acknowledging such flexibility, the SEC noted its expectation that policies be "tailored" based on an entity's operations and "reasonably designed" to address cybersecurity risks across its entire data infrastructure.[8]

---

[5] The SEC noted that advisers and funds can utilize the National Institute of Standards and Technology ("NIST") Cybersecurity Framework or available Cybersecurity and Infrastructure Security Agency ("CISA") guidance concerning certain "general elements" expected within adviser and fund cybersecurity policies.

[6] *Id*. at 20 n.30 ("Adviser information systems" is proposed to be defined as "information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.").

[7] *Id*. at 15, 17.

[8] *Id*. at 13, 16.

INCIDENT REPORTING

Consistent with the growing trend to require financial services to report a cybersecurity incident to regulatory agencies, the SEC proposed Advisers Act Rule 204-6.[9] This rule would require any adviser registered or required to be registered with the Commission to notify the Commission "promptly" – but in no event more than 48 hours – after having a "reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring."[10] A "significant adviser cybersecurity incident" would be defined as a "cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in (1) substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed."[11] The SEC did not propose a definition of "substantial harm"; instead, the agency offered a handful of examples.[12]

Such reporting would be done on the new proposed Form ADV-C and would cover incidents "affecting the adviser, or its fund or private fund clients."[13] The SEC recognized the need for the report to be confidential and not filed publicly. This new Form ADV-C would require an adviser to provide information regarding a significant cybersecurity incident through a series of check-the-box and fill-in-the-blank questions. Unlike other regulatory incident reporting obligations, Form ADV-C requests substantial details concerning the incident, including:

- Any actions or planned actions to recover from the incident;
- Whether data was stolen, altered accessed or used for an unauthorized purpose; and
- Whether the incident is covered under a cybersecurity insurance policy.[14]

---

[9] *Id*. at 46.

[10] The agency did not propose requirements that entities report to law enforcement. Instead, the SEC noted "[a]lthough an adviser's or a fund's initial focus may be on protecting its clients and investors, it may also wish to implement a process to determine promptly whether and how to contact local and Federal law enforcement authorities, such as the FBI, about an incident." *Id*. at 34 n.49.

[11] *Id*. at 47.

[12] *Id*. at 49 ("Substantial harm to an adviser as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or theft of intellectual property. Substantial harm to a client or an investor in a private fund as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or the theft of personally identifiable or proprietary information.").

[13] *Id*. at 14.

[14] *Id*. at 62.

Furthermore, under the proposed rules, advisers would need to amend any previously filed Form ADV-C "promptly, but in no event more than 48 hours after, information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident."[15] Thus, the short time period to report and the detailed information sought likely will result in multiple reports for a single significant adviser cybersecurity incident.

CYBERSECURITY RISK AND INCIDENTS DISCLOSURE

The SEC's suite of new rules also includes proposed amendments to Form ADV Part 2A for advisers and Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2 and S-6 for funds around cybersecurity risk and incident disclosure. According to the SEC, "[t]hese proposed amendments are designed to enhance investor protection by ensuring cybersecurity risk or incident-related information is available to increase understanding and insight into an adviser's or fund's cybersecurity history and risks."[16]

For investment advisers, the proposed amendments would add a new "Item 20" to Form ADV Part 2A entitled "Cybersecurity Risks and Incidents."[17] The brochure, which is an adviser's primary client-facing disclosure document, contains information about the investment adviser's business practices, fees, risks, conflicts of interest and disciplinary information. Advisers would be required to – in plain English – describe "cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize and address cybersecurity risks created by the nature and scope of their business."[18]

Advisers would be required to "identify the entity or entities affected, when the incidents were discovered and whether they are ongoing, whether any data was stolen, altered, or accessed or used for any other unauthorized purpose, the effect of the incident on the adviser's operations, and whether the adviser, or service provider has remediated or is currently remediating the incident."[19] Additionally, advisers would need to describe "any cybersecurity incidents that have occurred within the last two years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients."[20]

Furthermore, the SEC's proposed amendments to Advisers Act Rule 204-3 would require advisers to deliver interim brochure amendments to existing clients "promptly"

[15] *Id*. at 169.

[16] *Id*. at 60.

[17] *Id*. at 61.

[18] *Id*.

[19] *Id*. at 62.

[20] *Id*. at 170.

if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident.[21] The agency did not define "promptly" in the context of an updated brochure.[22]

BOOKS AND RECORDS

Finally, the SEC proposed that advisers and funds be subject to additional record-keeping requirements. For advisers, the SEC proposed amending Advisers Act Rule 204-2 – the books and records rule – which sets forth requirements for maintaining, making and retaining advertisements. If approved, advisers will be required to retain:

1. A copy of their cybersecurity policies and procedures formulated pursuant to proposed Rule 206(4)-9 that are in effect or were in effect at any time within the past five years;
2. A copy of the adviser's written report documenting the annual review of its cybersecurity policies and procedures pursuant to proposed Rule 206(4)-9;
3. A copy of any Form ADV-C filed by the adviser under Rule 204-6 in the last five years;
4. Records documenting the occurrence of any cybersecurity incident, as defined in Rule 206(4)-9(c), occurring in the last five years, including records related to any response and recovery from such an incident; and
5. Records documenting any risk assessment conducted pursuant to the cybersecurity policies and procedures required by Rule 206(4)-9(a)(1) in the last five years.[23]

KEY TAKEAWAYS

Chair Gensler's recent speech foreshadowed the SEC's efforts to impose new cybersecurity requirements for advisers and funds. The proposed rules will substantially impact such entities; if approved, many advisers and funds may have to develop more robust and comprehensive cybersecurity programs in a short time frame. Such comprehensive cybersecurity programs often require participation by multifunctional

[21] Currently, Rule 204-3(b) does not require advisers to deliver interim brochure amendments to existing clients unless the amendment includes certain disciplinary information in response to Item 9 Part 2A.

[22] In comparison, for filing the Form ADV-C with the SEC, the Commission proposal reads "promptly, but no later than 48 hours." As such, it is unclear if the agency views "promptly" in this context to be less than 48 hours.

[23] *Id*. at 44-45; Proposed Rule 38a-2 under the Investment Company Act includes similar proposed requirements.

teams, including personnel from information technology, internal audit, risk management and legal to ensure effective implementation, training, monitoring and testing.

In developing such a program, adviser and funds should be mindful of the following key takeaways:

- *Cybersecurity Risks or Incidents at Third Parties Could Result in Exposure to Advisers and Funds*: The SEC is proposing that advisers and funds consider the cybersecurity capabilities of third parties. The definition of "adviser information systems" – as reflected by the "or used by" prong of this definition – poses significant risks for advisers. To best achieve such third-party assessments, advisers and funds may need to consider documented cybersecurity due diligence reviews and contractual provisions containing specific cybersecurity and data privacy clauses. Without such documented efforts, the SEC could argue that advisers and funds failed to adequately assess a third-party's cybersecurity risks during the agency's ex post facto assessment following a third-party breach. Buried in the SEC's economic analysis of the rule, the Commission notes the following:

  > The proposed provisions require registrants to consider the cybersecurity risks resulting from their reliance on third-party service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing therein. Thus, the proposed requirements would affect a broad range of service providers: not only entities such as custodians, brokers, and valuation services, but also email providers, customer relationship management systems, cloud applications, and other technology vendors that meet this criterion. *Registrants would be required to document that such service providers implement and maintain appropriate measures to protect information of clients and investors and the systems hosting said information, pursuant to a written contract between the registrant and its service provider*.[24]

  Although the agency has previously sanctioned regulated entities for failure to comply with Regulation S-P in connection with breaches on third-party servers,[25] the requirement that advisers and funds assess such risks and document third-party cybersecurity risks would represent a significant regulatory expansion for these entities.

[24] *Id*. at 98 (emphasis added).

[25] https://www.sec.gov/litigation/admin/2015/ia-4204.pdf.

- *Uncertain Public Access to Cybersecurity Incident Reports*: In its discussion of the proposed rules, the SEC recognized the need for the report to be confidential.[26] The proposed rules, however, are silent concerning public access to cybersecurity incident reports through Freedom of Information Act ("FOIA") requests. The Office of the Comptroller of the Currency ("OCC"), Federal Reserve Board ("FRB") and Federal Deposit Insurance Corporation ("FDIC") recently addressed this FOIA concern during the comment process for its final rule requiring banking organization to notify its regulatory agency of cybersecurity incidents. The agencies recognized that FOIA requests for incident reports would be handled on a case-by-case basis. Alternatively, the proposed cyber incident report sharing provision within the National Defense Authorization Act that was debated in Congress last December explicitly exempted cybersecurity incident reports to the Cybersecurity and Infrastructure Security Agency ("CISA") from FOIA requests.[27] Given the lack of clarity, commenters may highlight this issue during the comment period which may cause the SEC to address the issue in its consideration of the final rules.

- *Near Real-Time Notification to Agency Creates Potential Risks*: As part of a growing trend, regulators are requiring cybersecurity incident notifications even when personal identifying information was neither accessed nor taken. Moreover, such requirements typically seek notification in short windows of time often while entities are in the early stage of responding to a cyber incident.

  The SEC's push for near real-time disclosures of certain incidents is not isolated. In the proposed rules, the SEC would require notification from advisers within 48 hours after they have a "reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring." The proposed rule does not define a "reasonable basis to conclude," although the Commission was clear that "reasonable basis" does not mean "after definitively concluding that an incident has occurred or is occurring." This means, conversely, that the Commission anticipates reporting before an entity definitively concludes that an incident is occurring. Under this proposal, entities will need to spend significant time and resources implementing protocols that allow for real-time analysis, incident response, remediation and notification. Even

[26] Proposed Rule at 59 ("Accordingly, our preliminary view is that Form ADV-C should be confidential given that public disclosure is neither necessary nor appropriate in the public interest for the protection of investors.").

[27] National Defense Authorization Act for Fiscal Year 2022, H.R.4350, 117th Cong., Senate Amdt No. 4813 to Senate Amdt 3867, Section 2235(c), https://www.congress.gov/congressional-record/2021/11/18/senate-section/article/S8456-1.

then, the notification trigger is uncertain and, as a result, may be subject to agency interpretation and hindsight in a regulatory action.

In addition, the SEC seeks a substantial level of details concerning the cybersecurity incident report, which raises litigation risks and privilege concerns. A cybersecurity incident may expose entities to consumer litigation, shareholder litigation and even third-party litigation. At 48 hours, entities may not be fully apprised of their litigation risks, but will be required to provide substantial information to the SEC that could result in inadvertent waiver of privileged information. Thus, while in the midst of a cybersecurity incident, advisers and funds will need to consider potential litigation risks associated with its disclosure to the SEC.

- *Ongoing Reporting Obligations Create Additional Burden*: Not only must advisers report to the Commission before determining if an incident has actually occurred, it must also continue updating the agency of "no event more than 48 hours after" it learns of "new material information about a previously reported incident is discovered" and "after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident." When combined with the obligation to report when there is only a "reasonable basis" to think an incident may have occurred, this could put the adviser in the position of consistently filing reports with the agency, an obligation that seemingly stretches beyond the bounds of almost anything currently required of public companies or regulated entities in other areas.

  Although the agency claims these "ongoing reporting obligations would further encourage advisers and funds to take the steps necessary to do so completely," it's unclear that such incentives don't already exist based on current federal and state regulations, and the obvious financial incentives.

  In addition, the Commission's proposed rules are flush with ambiguity around the reporting of cybersecurity incidents to the parties that these rules are meant to protect: the investors. Although the SEC rules contemplate reporting such incidents "promptly" to clients and investors, SEC Commissioner Allison Lee seized upon the proposed rule's lack of clarity around announcement time frames to adviser's clients.[28]

[28] Commissioner Allison Lee noted in a written statement: "These provisions raise a number of questions. For example, the proposal would require notification to the Commission of an incident within 48 hours, but the notification to an adviser's clients has no specific timeframe. Instead such notification would need to be made 'promptly.' Should investor notification be tied to a more discrete timeframe to ensure timeliness? And, what specific information do investors need to know about such incidents?"