Recent SEC EXAMS Risk Alert Highlights Key Considerations for Reg S-ID Compliance

December 15, 2022

On December 5, 2022, the Securities and Exchange Commission (the "SEC") Division of Examinations ("EXAMS") published a Risk Alert providing observations from recent examinations relating to investment adviser and broker-dealers' compliance with Regulation S-ID ("Reg S-ID"), also known as the Identity Theft Red Flags Rule (the "Red Flags Rule"). We previously wrote about the SEC's July 2022 charges against three financial institutions for violations of Rule 201 of Reg S-ID.

This week's Risk Alert underscores the SEC's continued focus on Reg S-ID compliance and view that registrants continue to demonstrate deficiencies in this area, and provides a useful roadmap for Reg S-ID compliance. EXAMS expects firms to establish and regularly update Reg S-ID policies and procedures that reflect the business model and particularized risks faced by each registrant and to engage in regular reevaluation of the Identity Theft Prevention Program (the "Program") in response to new and emerging identity theft risks.

MOST FREQUENTLY OBSERVED REG S-ID COMPLIANCE ISSUES

The Risk Alert covers the following three areas of Reg S-ID compliance where EXAMS identified deficiencies:

- Identification of covered accounts;
- Development and implementation of a written Program that meets all required elements; and
- Administration of a Program.

Identifying Covered Accounts

Firms have a continuing obligation to determine whether they offer accounts covered under Reg S-ID. EXAMS identified several areas where firms did not comply with their identification obligations:

- **Failure to identify covered accounts**. EXAMS observed some firms' failure to conduct required assessments to determine which, if any, accounts qualified as "covered accounts." Consequently, these firms failed to properly implement Programs.

- **Failure to identify new and additional covered accounts**. EXAMS observed that some firms initially identified covered accounts as one category of accounts that they offered. However, they ultimately failed to conduct periodic assessments—either at all or in a manner that sufficiently identified all categories of new accounts that were also "covered accounts." EXAMS observed that firms merging with other entities should conduct a reassessment to determine whether to include new accounts in the Program. Additionally, the determination and reassessment of covered accounts should include online accounts, retirement accounts and other special purpose accounts. EXAMS also underscored that firms should maintain documentation of their analysis of covered accounts and noted that while such documentation is not required by Reg S-ID, EXAMS can assist firms in identifying the basis for their determination to auditors and regulators.

- **Failure to conduct risk assessments**. Even where firms periodically identified covered accounts, firms sometimes failed to conduct a risk assessment in which they assess the methods for opening, maintaining, accessing and closing accounts, as well as the firm's prior experiences with identity theft. EXAMS flagged that the absence of risk assessments prevented some firms from identifying certain covered accounts, which limited firms' ability to develop controls relevant to their red flags. As required by Reg S-ID, firms should conduct such risk assessments periodically to determine whether they need to include additional accounts in the scope of "covered accounts" as a result of changes to account types or features. Such risk assessments should in turn identify particular red flags based on such changes.

Developing and Implementing a Written Program That Meets All Required Elements

Regulation S-ID requires that firms create a written Program appropriate for that specific firm that is based on the firm's size, activities and complexity of transactions. The Program must cover all required elements of the regulation, enumerating policies and procedures to identify, detect and respond to red flags of identity theft. The Program should include reasonable policies and procedures to ensure that it is updated regularly to be consistent with changes in the threat landscape in terms of risks to

customers and the safety and soundness of the registrant. EXAMS highlighted several issues related to Program implementation:

- **Failure to tailor a Program to the business**. Using a Reg S-ID template with fill-in-the-blanks is insufficient, as is restating the Regulation as the firm's policy. Firms must design a Program that is tailored to their particular business model.

- **Failure to identify red flags**. EXAMS found that firms lacked reasonable policies and procedures to spot red flags, which are patterns, practices or specific activities that indicate possible identity theft. Some firms did not include any specific identified red flags for their Programs, while other firms identified red flags that were not relevant to their business models. Firms should take care to assess relevant red flags for their covered accounts and add additional red flags to their Programs as appropriate (for example, identifying new identities or services being used for identity theft).

- **Failure to detect and respond to red flags**. Firms relied too heavily on preexisting policies and procedures, such as anti-money laundering procedures, which were not designed to combat identity theft. EXAMS found that firms either did not detect or did not adequately respond to instances of identity theft because they did not have policies and procedures tailored to relevant red flags. While a firm might maintain other policies related to identity theft prevention, firms should incorporate these procedures directly or by reference into their Programs—and to the extent that other policies and procedures are incorporated by reference into the Program, they should cover all of the required elements of Reg S-ID.

- **Failure to periodically update Programs**. The Regulation requires that firms update their Programs to reflect developments in the firm and identity theft risks. When undergoing business changes or reorganizations, firms should take care to make relevant Program changes or to approve a new Program for new lines of business.

Administering a Program

Firms are required to take four steps to provide for the continued administration of Reg S-ID. *First*, firms should obtain approval of their initial written Program from either an appropriate committee of the Board of Directors (or senior management if the firm lacks a Board). *Second*, the Board or senior management needs to be involved in administering the Program. *Third*, the appropriate staff should be trained on the Program. *Fourth*, the firm should conduct oversight of service provider arrangements for compliance. EXAMS noticed several areas where firms failed to meet these obligations:

- **Failure to provide sufficient information to the Board or senior management**. Some firms were not providing the Board or senior management with any reports or with insufficient reports. Reports should be sufficiently detailed to allow the Board or senior management to evaluate the effectiveness of the Program.

- **Failure to provide adequate training**. Firms sometimes failed to assess which employees need training on identity theft prevention and/or provided insufficient training. Firms should conduct comprehensive training as well as periodically determine which employees should be trained.

- **Failure to evaluate controls of service providers**. When a firm relies on an outside service provider to perform activities related to covered accounts, that outside service provider should also have adequate identity theft prevention controls. EXAMS underscored that firms should evaluate the identity theft controls in place at third-party service providers.

You can find our previous coverage of SEC enforcement actions in data- and cybersecurity-related matters (here, here, here, here, and here).

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise Law Clerk Charlotte Blatt for her work on this Debevoise Data Blog post.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

Noah L. Schwartz
nlschwartz@debevoise.com

SAN FRANCISCO

Kristin A. Snyder
kasnyder@debevoise.com

Lessons from the SEC's Most Recent Reg S-P Action

October 6, 2022

On September 20, 2022, the SEC announced settled charges and the imposition of a $35 million penalty against a dually registered investment adviser and broker-dealer (the "Firm") for violations of Regulation S-P ("Reg S-P"). The SEC found that the Firm violated Reg S-P's requirements for registrants to adopt written policies and procedures to safeguard customer records and information (the "Safeguards Rule") and to take reasonable measures to protect against unauthorized access or use of consumer report information and records in connection with disposal of this material (the "Disposal Rule").

This matter is the first SEC enforcement action under Reg S-P's Disposal Rule and signals that we can expect to see future examinations, investigations, and settlements focused on the inadequate disposal of customer PII and consumer report information. The settlement also underscores that Reg S-P enforcement remains a priority for the Commission, which as discussed in our Data Blog post, brought a series of Reg S-P actions just last year.

THE FIRM'S DATA DECOMMISSIONING FAILURES

Facts

The SEC's Order details a series of failures to protect and dispose of consumer information, including personally identifying information ("PII"), in connection with the Firm's decommissioning of data centers, local branch servers, and other projects. Much of the relevant conduct detailed in the SEC's Order involved the Firm's lack of diligence in selecting and effectively monitoring a vendor retained to remove, destroy, or delete the data contained on its devices.

According to the Order, the Firm hired a moving company (the "Moving Company") to decommission its two primary data centers where some of the devices contained unencrypted PII. The SEC described the Moving Company as "strictly a moving company" that provided "local trucking, storage, and long distance moving" services but

lacked any experience with data destruction. The SEC found that the Firm's oversight of the Moving Company and the disposal process was lacking. The Moving Company hired a sub-vendor that was not approved by the Firm, and the Firm later missed signs that the Moving Company replaced that sub-vendor without its approval and that the sub-vendor was not properly carrying out the data destruction.

As a result, the SEC found that the Firm had unknowingly sold IT assets, including unwiped hard drives, which contained thousands of pieces of customer PII.

With respect to the Firm's server decommissioning, the SEC found that the Firm failed to document its work disposing of 500 server devices via Certificates of Destruction and evidence of the chain of custody. According to the SEC's Order, the Firm later realized that 42 of those devices had gone missing and that not all of the data on those devices had been encrypted. The SEC also found that in other projects, the Firm, through the Moving Company and its sub-vendor, did not adhere to its heightened internal requirements for disposal of backup tapes.

Violations

Failure to Adopt Written Policies and Procedures for Decommissioning.
The SEC found that the Firm failed to adopt written policies and procedures that identified the high level of risk associated with device decommissioning and relating to the resale of old or decommissioned devices.

Failure to Adopt Reasonably Designed Policies and Procedures for Vendors.
The SEC found that the Firm's written policies and procedures were not reasonably designed because they failed to ensure the use of a qualified vendor for the decommissioning projects. The Firm retained the Moving Company even though it was aware—as documented in its internal risk assessment—that the Moving Company was not capable of carrying out the required work. The Firm's policies and procedures also did not ensure that it reviewed and approved sub-vendors and would be subsequently made aware of a change in sub-vendors.

The SEC's Order found that the Firm's policies and procedures also failed to provide sufficient monitoring of the Moving Company's performance, even though it was aware of problems involving its record maintenance.

Failure to Take Reasonable Measures to Protect Customer PII or Consumer Report Information in Connection with Decommissioning Data-Bearing Devices.
The SEC found that the Firm did not follow its own requirements for documenting the destruction of data (including consumer PII or consumer report information) and failed to implement and monitor compliance with its own policies and procedures for the destruction of backup tapes (even though these policies and procedures recognized the

"significant risk" associated with them). Here, the SEC noted that the Firm failed to comply with its policies and procedures in connection with the destruction of 40,000 backup tapes handled by the Moving Company.

ENFORCEMENT'S CONTINUED FOCUS ON DATA SECURITY AND VENDOR MANAGEMENT

This latest entry in the rapidly growing roster of the SEC's cyber and data security enforcement actions illustrates that the Commission is prepared to issue significant settlements to prevent investor harm resulting from data handling and disposal failures at registrants. Director of Enforcement Gurbir Grewal underscored these priorities by declaring in the press release for the settlement that the "failures in this case are astonishing" and that insufficient safeguards for customer data can "have disastrous consequences for investors. Today's action sends a clear message to financial institutions that they must take seriously their obligation to safeguard such data." The significant size of the penalty underscores the importance of these issues to the SEC, who is not the only regulator with oversight over the security of customer PII or the disposal of consumer report information. The CFPB and FTC have issued Safeguards Rules covering entities subject to the Gramm-Leach-Bliley Act under their jurisdiction. The FTC has also issued a Disposal Rule under the Fair and Accurate Credit Transactions Act that applies to any person subject to the FTC's jurisdiction that, for a business purpose, maintains or otherwise possesses consumer information. Disposal of PII is also a component of New York's SHIELD Act and NY DFS Part 500.

The case also demonstrates the SEC's focus on the role that third-party vendors play in protecting consumer data and builds upon the SEC's 2018 enforcement action against Voya Financial Advisors for Safeguards Rule violations in which the Commission found, in relevant part, that Voya's policies and procedures with respect to its independent contractors were not reasonably designed and, in some cases, not applied to the systems used by independent contractors at all.

KEY TAKEAWAYS

The settlement provides several important lessons for registrants—and others that handle covered data—on compliance with Reg S-P and, in particular, the Disposal Rule:

- ***Address High-Risk Devices in Data and Device Destruction Policies and Procedures***. Registrants and others subject to Safeguards and Disposal Rules should consider addressing the risk stemming from the improper safeguarding and disposal of data

that may contain consumer PII or consumer report information. Establishing specifically heightened standards for such data in internal policies and procedures can help prevent mishandling of that data.

- ***Vendor Diligence and Selection***. Registrants and others subject to Safeguards and Disposal Rules should consider including in their policies and procedures requirements for thorough vetting of potential vendors and sub-vendors. This review would include a risk assessment and a determination that the vendor is capable and experienced in handling and disposing of consumer PII and consumer report data in a manner compliant with Reg S-P. Policies and procedures governing vendor risk assessments should ideally have built-in triggers to escalate issues. The SEC found that the Moving Company's lack of experience in handling data disposal was flagged in a risk assessment but did not affect their selection.

- ***Continued Oversight of Vendors***. Assurance from vendors about the handling and destruction of consumer PII and consumer report information may not be sufficient for Reg S-P compliance. The SEC found that the Firm had the capability to monitor the Moving Company's handling of its asset inventory, yet chose not to exercise that supervisory responsibility. Registrants and others subject to Safeguards and Disposal Rules may wish to create processes to ensure periodic oversight and check-ins with vendors in order to verify that removal, transport, and/or destruction of data is being executed on an ongoing basis consistent with contractual terms as well as with Safeguards and Disposal Rules requirements. This oversight could encompass periodic review and verification of documentation provided by a vendor related to handling and disposal of consumer PII or consumer report information. The SEC found that if the Firm had reviewed the documentation provided by the Moving Company's replacement sub-vendor, it would have spotted a number of issues, including that certain hard drives were not being wiped of data.

- ***Maintain and Periodically Update Asset Inventories***. Registrants and others subject to Safeguards and Disposal Rules should consider including in their policies and procedures timelines according to which asset inventories should be examined and updated, noting which assets contain sensitive information, including consumer PII or consumer report information. Keeping inventories and classifications current will prevent headaches in the transport and decommissioning of devices since devices will be handled in line with their respective level of sensitivity.

- ***Contemporaneously Document Adherence to Policies and Procedures***. If the SEC commences an investigation or examination, contemporaneous documentation about how policies and procedures were followed will be useful for a registrant to share with the Staff. Given the Commission's scrutiny of vendor management—a context in which a registrant and others subject to Safeguards and Disposal Rules

necessarily have less control of the process—comprehensive documentation will better position a registrant and others subject to Safeguards and Disposal Rules for examination or enforcement response.

* * *

Please do not hesitate to contact us with any questions. To subscribe to our Data Blog, please click here.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

Scott M. Caravello
smcaravello@debevoise.com

SAN FRANCISCO

Kristin A. Snyder
kasnyder@debevoise.com

Recent SEC Enforcement Actions Signal Key Lessons for Reg S-ID Compliance

August 3, 2022

On July 27, 2022, the Securities and Exchange Commission ("SEC") separately charged three financial institutions with violations of Rule 201 of Regulation S-ID ("Reg S-ID"), also known as the Identity Theft Red Flags Rule ("Red Flags Rule"). The announcement of multiple Reg S-ID enforcement settlements (all of which were investigated by the SEC's recently-expanded Crypto Assets and Cyber Unit and originated from referrals from the Division of Examinations) highlights the SEC's agency-wide focus on Reg S-ID compliance. Notably, these are the first Reg S-ID cases the SEC has brought since 2018, when the Commission brought its first-ever Reg S-ID action.

The SEC's orders detail numerous deficiencies in each firm's Identity Theft Prevention Program ("ITPP"), provide registrants with an outline of the Commission's expectations for compliance with Reg S-ID, and underscore the Commission's increasing scrutiny of cybersecurity deficiencies in the securities marketplace.

The orders establish that registrants must craft ITPPs that are particularized to each individual firm and updated to cover new risks. Given the evolving identity theft threat landscape, firms should consider building cross-functional teams drawing resources from the business, compliance, legal, privacy, and cyber areas to address these cybersecurity risks.

Overview of Reg S-ID's Requirements

Rule 201 of Reg S-ID requires financial institutions and creditors to periodically determine whether they offer or maintain "covered accounts," which are defined as (i) accounts that are offered or maintained primarily for personal, family, or household purposes and involve or are designed to permit multiple payments or transactions, and (ii) any other account for which there is a reasonably foreseeable risk of identity theft.

A financial institution or creditor that offers or maintains covered accounts must develop and implement a written identity theft prevention program. The program must:

- Be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account;
- Be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities;
- Include reasonable policies and procedures to identify red flags for covered accounts, incorporate those red flags into the program, detect red flags that have been incorporated, and respond appropriately to any red flags that are detected; and
- Include reasonable policies and procedures to ensure the program and any red flags determined to be relevant are updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

The financial institution or creditor must also:

- Provide for the continued administration of the program;
- Obtain approval of the initial written program from its board of directors (or an appropriate committee thereof);
- Involve the board (or an appropriate committee of the board or designee from senior management) in the oversight, development, implementation, and administration of the program;
- Train staff, as necessary, to effectively implement the identity theft prevention program; and
- Exercise appropriate and effective oversight of service provider arrangements.

Appendix A to Reg S-ID contains criteria that each financial institution or creditor should consider including in its program, as appropriate, such as categories and examples of red flags, factors to consider in updating a program, and guidelines for oversight of service providers.

The July 27, 2022 Orders

The three July 27, 2022 orders stem from similar findings by the SEC. Two of the charged firms are global financial services institutions with dually-registered broker-

dealers and investment advisers. The third is a broker-dealer that offers online brokerage services to retail customers.

The orders relate to violations between 2017 and 2019. None of the orders detail any actual loss or identity theft to customers attributable to the violations. Instead, the orders find that each company failed to maintain an adequate program, as required by the regulations. Without admitting or denying the SEC's findings, the firms agreed to cease and desist from future violations; censures; and to pay penalties ranging from $425,000 to $1.2 million. The settlements are also notable because they originated in referrals from the Division of Examinations to the Division of Enforcement, illustrating that cybersecurity remains a priority across the entire Commission.

SEC's Focus on Reg S-ID and Cybersecurity Enforcement

The SEC settlements noted that although all three companies had ITPPs, they failed to tailor their programs to their respective businesses and to update the programs in a timely manner. Consequently, each firm, according the SEC, failed to satisfy several requirements of Reg S-ID.

All three charged firms had programs that the SEC views as failing to include reasonable policies and procedures to (1) identify, incorporate, detect, and respond appropriately to red flags, and (2) ensure their programs were updated periodically to reflect changing risks. The SEC faulted the firms' respective ITPPs for simply restating the general legal requirements of Reg S-ID without providing particularized guidance for identifying, detecting, and responding to red flags, which was tailored to the firms' specific business models. The SEC also found failures in: the oversight of service providers; training of staff to implement ITPPs; reporting to the board of directors (when the board was charged with supervising the ITPP); the periodic review of new or existing types of customer accounts to ascertain whether they were "covered accounts"; and ITPP updates to reflect emerging cybersecurity risks.

The July 2022 actions mark only the second time that the SEC has brought charges for violating Reg S-ID. In September 2018, the SEC charged a dually registered broker-dealer and investment adviser with violating Reg S-ID and the Safeguards Rule of Regulation S-P in connection with a cyber intrusion that compromised customers' personal information. Similar to the July 2022 Reg S-ID settlements, the SEC found that the firm did not review and update its ITPP in response to changes in risks, did not provide adequate training to staff, did not ensure adequate board oversight of the program, and did not have reasonable policies and procedures to respond to red flags. However, it is noteworthy that in the 2018 matter, there was an underlying identity

theft that highlighted the deficiencies to the SEC, whereas in the present matters, no instances of identity theft were discussed in the orders—demonstrating that the Commission will not hesitate to charge cybersecurity violations, even in the absence of actual harm to investors.

Key Takeaways from SEC Enforcement for Reg S-ID Compliance

The trio of Reg S-ID settlements underscores that SEC registrants should regularly review their written ITPPs for compliance with Reg S-ID. Important considerations include:

- **Identifying and Incorporating Red Flags in the ITPP Tailored to Each Firm's Risks:** Firms should re-examine their ITPPs to ensure they contain reasonable policies and procedures to identify and incorporate particularized red flags relevant to their institutions or their own experiences with identity theft risks. For example, although Appendix A to Reg S-ID contains a lengthy list of potential identity theft red flags, a firm should not unthinkingly adopt this list wholesale, but could instead identify and incorporate only those red flags that the firm considers relevant to its business model. Additionally, where a firm does not obtain and review consumer reports in connection with opening covered accounts, its ITPP should not reference red flags related to information received from consumer reporting agencies. On the other hand, where a firm encounters specific forms of social engineering or account-takeover fraud, the policies could be updated to reflect and address those risks. In turn, in determining relevant categories of red flags, a firm should look to factors applicable to its own business, such as the types of covered accounts it offers or maintains, methods to open and access accounts, and prior experiences with identity theft.

- **Detecting and Responding to Red Flags:** Firms should consider whether their ITPPs contain reasonable policies and procedures to detect and respond appropriately to red flags. For example, potentially appropriate responses to red flags include declining to open a new account and notifying law enforcement. Firms should consider providing specific steps for employees to undertake in addressing red flags.

- **Periodic Updates Based on Changing Risks:** Firms should consider whether their ITPPs contain reasonable policies and procedures to ensure periodic updates to reflect changing risks. The SEC settlements emphasized the "significant changes in external cybersecurity risks related to identity theft" in recent years. Firms that have not regularly made material changes to ITPPs to reflect the emerging cybersecurity

risk landscape should consider assessing evolving identity theft-related risks and updating their programs accordingly. Further, if a firm's ITPP states that the firm will review and update it periodically, the policy could also describe the frequency of review and the mechanics of policy updates.

- **Evaluating "Covered Accounts":** Firms should consider developing, maintaining, and implementing policies and procedures for determining whether they maintain or offer "covered accounts" and for identifying new types of covered accounts offered. The SEC settlements suggest that firms should identity red flags based on the types of covered accounts that the firm specifically offers or maintains, and should conduct risk assessments or other evaluations to determine the types of accounts it offers or maintains.

- **Cross-Functional Compliance:** The process of creating and updating an ITPP in order to meet the particularized risks of a firm benefits from input from a cross-functional team of stakeholders. For example: customer service representatives can share the experiences they have with customers (and fraudsters); cybersecurity teams can identify new methods of account takeover fraud; privacy teams can share experiences from breach notifications; and the law and compliance teams can bring together updates. A cross-functional team can help facilitate ongoing compliance, particularly at global financial institutions where relevant responsibilities and duties may be shared across multiple groups.

- **Board Involvement:** ITPPs should address involvement from the board of directors (or a committee thereof or a designee from senior management, as appropriate). Specifically, the firm should consider providing the board with reports specific to the program and compliance with Reg S-ID. Such reports could include sufficient information about the program's effectiveness, significant identity theft-related incidents and management's responses, and metrics related to identity theft at the firm. Moreover, the firm should consider documenting any board-level discussions about compliance with Reg S-ID.

- **Staff Training:** Firms should consider providing training to staff on effective implementation of the ITPP, including training on identifying, detecting, monitoring, and responding to red flags.

- **Oversight of Service Providers:** Firms should consider evaluating whether they exercise appropriate and effective oversight of service providers, including whether their activities comply with reasonable policies and procedures to detect, prevent, and mitigate identity theft.

Finally, even if a firm takes actions to respond to actual incidents of identity theft, its written ITPP should include those actions in its policies and procedures. And importantly, where a firm has reasonable policies and procedures in place, it should make sure to follow them.

You can find our previous coverage of SEC enforcement actions in data- and cybersecurity-related matters (here, here, here, here, and here).

* * *

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise Law Clerk Lily Coad for her work on this Debevoise Data Blog.

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Charu A. Chandrasekhar
cachandrasekhar@debevoise.com

Noah L. Schwartz
nlschwartz@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

SAN FRANCISCO

Kristin A. Snyder
kasnyder@debevoise.com

Four Takeaways from the SEC's Proposed Cybersecurity Rules

February 17, 2022

On February 9, 2022, the SEC released its much-anticipated proposed rules relating to cybersecurity risk management, incident reporting, and disclosure for investment advisers and funds. Many of the proposals follow the trends that members of the Debevoise Data Strategy & Security and White Collar & Regulatory Defense practice groups discussed during a November 2021 webcast on the SEC's Cybersecurity Year in Review, as well as in our prior Data Blog posts (here and here).

Chair Gensler recently emphasized that cybersecurity rulemaking in this area is one of his priorities, and placed particular emphasis on establishing standards for cybersecurity hygiene and incident reporting for registrants. The proposed rules, which are the most detailed cybersecurity rules that Chair Gensler's SEC has issued thus far, reflect the SEC's intense attention to cybersecurity risk and its willingness to deploy the full scope of its regulatory authority to promulgate standards that address this risk.

These proposed rules would impose significant new requirements on registered investment advisers and funds, and are generally consistent with cybersecurity requirements imposed on other companies by New York's Part 500 Cybersecurity Regulation and the Federal Trade Commission's updated Safeguards Rule.

Key Requirements under the Proposed Rules

Cybersecurity Risk Management Policies & Procedures

The proposed rules would require advisers and funds to adopt and implement policies and procedures that are "reasonably designed" to address cybersecurity risks. There are several "general elements" that advisers and funds will need to address in their cybersecurity policies and procedures, including risk assessment practices, user security and access, preventing unauthorized access to funds, threat and vulnerability management, and incident response and recovery. The proposed rules require advisers and funds, on an annual basis, to: (1) review and assess the design and effectiveness of their cybersecurity policies and procedures; and (2) prepare a report describing the

review, explaining the results, documenting any incident that has occurred since the last report, and discussing any material changes to the policies and procedures since the last report.

The proposed rules also add requirements relating to board oversight and recordkeeping. Under Proposed Rule 38a-2, registered funds would be required to have their boards, including a majority of its independent directors, (1) approve their cybersecurity policies and procedures, and (2) review the annual report.

Incident Reporting

The proposed rules would also require advisers, "including on behalf of a client that is a registered investment company or business development company, or a private fund" (collectively, "covered clients"), to report any significant cybersecurity incidents, which are defined as any event that (1) "significantly disrupts or degrades the adviser's" or private fund client's "ability to maintain critical operations" or (2) "leads to the unauthorized access or use of adviser information" resulting in substantial harm to the adviser, or substantial harm to a client, or an investor in a private fund, whose information was accessed. Advisers, on behalf of themselves and their covered clients, must report to the SEC within 48 hours from when they have a reasonable basis to believe such an incident has occurred.

Advisers must use the new proposed Form ADV-C for incident notification to the SEC. The notification must include a detailed description of the nature and scope of the incident and any disclosures about it. Advisers will be expected to update any previously submitted Forms ADV-C when there has been a material change in facts. The proposed rule states that submitted Forms ADV-C will remain confidential and not be disclosed to the general public. However, the proposed rules do not address whether the ADV-C filing would be exempt from FOIA.

Disclosure Obligations for Advisers

The proposed rules would also amend Form ADV Part 2A for advisers to include disclosure of cybersecurity risks and incidents that could materially affect the advisory relationship with current and prospective clients. The amendment would require that advisers describe, in plain English, the cybersecurity risks that could materially affect the services they offer and how they plan to assess and address those risks. If adopted, the disclosures must include information about the likelihood and extent to which the cybersecurity risk or incident: (1) could occur and what safeguards are in place to prevent it; (2) could or has disrupted the adviser's ability to provide services; (3) could or has resulted in the loss or compromise of sensitive data; and (4) has or could harm clients.

The proposed amendments would also require advisers to describe any significant cybersecurity incidents that have occurred within the last two fiscal years and require advisers to deliver interim brochure amendments to clients if (1) the adviser was subject to a cybersecurity incident after the dissemination of its brochure, or (2) the information already disclosed in its brochure about an incident materially changes based on new discoveries.

Disclosure Obligations for Funds

Under the proposed rules, changes would be made to Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for funds to report significant cybersecurity incidents and risks, similar to the required disclosures for advisers. The rules propose amendments to funds' registration forms that would require a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years, and expands the definition of "principal risks" of investing in the fund to include cybersecurity risks and requires disclosure of such in fund registration statements. To the extent that cybersecurity incidents occur after the filing of a fund's registration forms and this alters the material position or risks involved with the fund, the fund must then file a supplement to the Commission.

Key Takeaways

Prepare for 48-Hour Breach Notice Deadline

Advisers may find it challenging to meet the strict 48-hour reporting timeline requirements set out by the proposed rules. Many companies have struggled to meet the longer 72-hour breach notification deadlines under the NYDFS Part 500 and GDPR. Having clear protocols for escalating incidents, drafting the notifications, and obtaining the necessary approvals can make the difference between (1) meeting tight notification deadlines and gaining credibility with the applicable regulator, and (2) missing the deadline and starting off having to explain to the regulator why the notification was late, which can undermine the regulator's view of the overall competence of the response. Advisers can learn from banks that are preparing for the new 36-hour reporting requirement, which have started implementing such protocols, including:

- Who is Covered -- Determining which entities in their group are subject to the new notification deadline, and if it only applies to some entities, assessing which data, information systems, and employees are associated with the covered entities.

- Who is Responsible -- Determining who the person responsible for making the notification, and who else, if anyone, must approve the notification before it is made.

It may be prudent to designate more than one person for each of these roles, in case someone is unavailable.

- Prompt Escalation -- Determining which incidents may trigger the short-deadline notification requirement and therefore should be escalated to the persons responsible for that notification, as well as who should be making that escalation.

- Notification Template -- Creating a sample notification, so that the actual notification does not need to be drafted from scratch during an incident.

Adopt, Implement, and Test Policies and Procedures

The proposed rules expand the policies and procedures obligations for advisers and registered funds. Proposed rules 206(4)-9 and 38a-2 would require advisers and registered funds to establish and implement cybersecurity policies and procedures that are "reasonably designed to mitigate cybersecurity risk," including risk assessment, standards for user security and access, information protection, threat and vulnerability management, and cybersecurity incident response and recovery. The proposed rules also provide very specific guidance on multiple elements of an expected cybersecurity risk and incident response program; while preexisting policies and procedures may include some of these components, they must now include all of them. Moreover, regular testing to ensure sufficient implementation will be crucial to effective compliance with the SEC's objectives of cybersecurity risk mitigation and compliance. Targeting policies and procedures violations has been a longstanding enforcement approach for the SEC (see First American), and the proposed rules provide a clear "hook" for doing so in the SEC's priority area of cybersecurity.

Disclosures and Evidence Preservation

The proposed rules emphasize the importance of clear and accurate disclosures regarding cybersecurity risk and incidents to investors and the SEC, formalizing takeaways from the SEC's 2021 enforcement actions against Pearson and First American as well as the priorities emphasized by Chair Gensler. As it has in the past, we can expect that the SEC will use the proposed rules once enacted to scrutinize cybersecurity-related disclosures and recordkeeping violations through exams and enforcement actions. Companies should ensure that their disclosures are not only accurate, but are also supported by objective evidence and documentation, which will require some thoughtful analysis as to which aspects of the investigation the company wishes to assert privilege.

Incident Response Planning

Through these proposed rules, the SEC has stressed the importance of maintaining continued operations in the event of an incident. Advisers and funds should therefore review their incident response plans and business continuity plans, and consider testing those plans through a tabletop exercises. Given that the proposed rules expand notification obligations of advisers and funds to include incidents affecting private fund and BDC clients' systems or information, these tabletop exercises can test escalation of incidents and engagement of all the relevant players in the incident response process.

We will continue to track and blog on these important updates. Public comments are open until at least April 9, 2022.

* * *

The Debevoise Data Portal is now available for clients to help them quickly assess and comply with their state, federal, and international breach notification obligations, as well as their substantive cybersecurity and AI legal obligations.

To subscribe to our Data Blog, please click here.

The authors would like to thank Linda Lin, a Debevoise law clerk, for her contributions to this post.

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

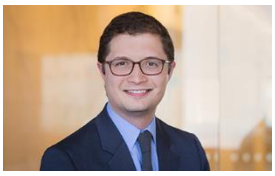
Matthew C. Rametta
mcrametta@debevoise.com

WASHINGTON, DC

Luke Dembosky
ldembosky@debevoise.com

Julie M. Riewe
jriewe@debevoise.com

SAN FRANCISCO



Christopher S. Ford
csford@debevoise.com

H Jacqueline Brehmer
hjbrehmer@debevoise.com