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