COMPLIANCE CORNER

Privacy and Cybersecurity: How Advisers Must Protect their Clients' Most Valuable Asset

By Paul M. Miller and Casey J. Jennings, Seward & Kissel LLP*

Introduction

Investment advisers well understand their responsibility for preserving such treasured client assets as family legacies, life savings, college tuition, and retirement. But investments are not the only invaluable possessions entrusted to the care of advisers. In fact, the most important item an adviser stewards may be a client's personal data – that information characterizing a client's very personhood, and which, if used in the wrong way, can wreak as much havoc on a client as poor investment advice.

Client personal data is a target. Data breaches in 2021 hit an all-time high, and if long-term trends continue, 2022 will break that record. In 2021, the Identity Theft Resource Center identified almost 2,000 significant data breaches affecting almost 300 million individuals. Perhaps counterintuitively, the total number of victims dropped in 2021, the result of more targeted attacks as criminals altered their strategy from *accumulating* stolen data (as had been their main strategy) to *exploiting* stolen data. Relatedly, identity theft is a significant problem. A recent survey by Javelin found that the identities of 15 million individuals were stolen, with losses in 2021 increasing by 79% over the prior year to $24 billion.

It is no surprise then that the SEC and its staff are increasingly focused on data issues, recently proposing new regulations governing cybersecurity and data privacy and protection, issuing two risk alerts highlighting the SEC staff's concerns in 2020, and bringing multiple data-related enforcement actions.

Paul M. Miller

Casey J. Jennings

"[T]he Cybersecurity Proposal would require an adviser to disclose cybersecurity risks and incidents to clients. An adviser would do so through new Item 20 of Form ADV Part 2A, which would describe the adviser's cybersecurity risks and how the adviser addresses them. . . [It] would require advisers to file a report with the SEC on new Form ADV-C within 48 hours after a 'significant' data breach and file an amendment after resolving such an incident."

In this article, we summarize an adviser's myriad and evolving federal, state, and cross-border regulatory obligations with respect to client data. Adviser obligations fall within three categories, discussed in turn below: (1) client disclosures; (2) written policies and procedures; and (3) preparedness and response.

Applicable Laws

An adviser's data processing activities are governed by the multiple federal and state laws that often overlap in applicability and requirements.

The Gramm-Leach-Bliley Act of 1999 ("**GLBA**"), as implemented by Regulation S-P, applies to "non-public personal information" ("**NPI**") processed by advisers. NPI is any data not otherwise publicly available that an adviser obtains in connection with a consumer financial product or service. Nearly all of an adviser's client data is NPI covered by Regulation S-P, but data an adviser collects from its website, about an adviser's employees, or about prospective clients (such as email addresses collected at a roadshow) is not NPI and thus is not covered by Regulation S-P. Regulation S-ID, which also applies to advisers, requires them to adopt a written identity theft prevention program designed to identify relevant types of identity theft red flags and to detect and respond to the detected red flags.

Advisers may be subject to the Cali-

Continued on page 9

Continued from page 8

fornia Consumer Privacy Act of 2018 ("**CCPA**"), which became effective January 1, 2020. The CCPA applies to companies that do business in California (even online) and either (1) have gross annual revenue of at least $25 million; (2) annually buy, receive, or sell the personal information of 50,000 or more California consumers; or (3) derive 50% or more of their revenue from selling California consumers' personal information. Although advisers are not excepted from the requirements of the CCPA, the CCPA does not apply its protections to data processed "pursuant to" the GLBA. Accordingly, client data is not subject to the CCPA, but website data, employee data, and prospective client data – all of which is excluded from the GLBA – is subject to the CCPA. The California Privacy Rights Act ("**CPRA**"), which will amend the CCPA effective January 1, 2023, adds several new prescriptive requirements.

Colorado, Utah, Virginia, and Washington have recently adopted privacy laws, but those laws exempt financial institutions regulated under the GLBA, including advisers. However, state data breach notification laws do apply to advisers.

Advisers must comply with the Investment Advisers Act of 1940 (the "**Advisers Act**") and rules adopted thereunder. As noted above, the SEC proposed new rules in February 2022 under both the Advisers Act and the Investment Company Act of 1940 (the "**Cybersecurity Proposal**") which, according to SEC Chair **Gary Gensler**, are "designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers against cybersecurity threats and attacks." The SEC has not yet adopted the proposed rules but is expected to.

Finally, advisers with European clients are subject to the European Union's General Data Protection Regulation ("**GDPR**"), which became effective in May 2018.

"[U]nder GDPR, regulator notification is step one, and a severity threshold determines whether clients should be notified; in the U.S., client notification is step one, and a severity threshold determines whether regulators should be notified."

Client Disclosures

Regulation S-P Notices

Regulation S-P requires advisers to provide clients a "clear and conspicuous" privacy notice in writing before collection describing (1) the data collected by the adviser, (2) with whom the data is shared, and (3) how the adviser protects the data. Regulation S-P contains a model privacy notice, the use of which makes an adviser eligible for a safe harbor from enforcement.

If it shares NPI with non-affiliated third parties, the adviser must provide the client the right to opt-out of such sharing unless an exception applies. Exceptions may apply to data sharing (1) necessary for effecting a transaction, or processing or servicing a financial product or a service requested or authorized by a client; (2) to prevent fraud, respond to judicial process or regulatory authorities or comply with a governmental investigation or a subpoena, or comply with federal, state, or local laws; (3) to third-party service providers; or (4) for joint marketing with other financial institutions (subject to limitations imposed by Regulation S-AM).

CCPA Notices

Like Regulation S-P, the CCPA requires advisers subject to the law to provide a privacy notice before collecting data from an individual, but the required notice is significantly more detailed than that required under Regulation S-P. The notice must describe the categories of data collected, the method(s) of collection, whether the data is shared or sold, the third parties with whom the data is shared or to whom it is sold, and what rights individuals have under the CCPA (including the right to stop the sharing or sale of data and the right to order the adviser to delete certain of their data). Additionally, if an adviser subject to the CCPA sells data to third parties, it must have a prominent "Do Not Sell" button on its website.

Employees whose data is protected under the CCPA are also entitled to a privacy notice, though employees do not have the same substantive data rights as non-employees.

Proposed Additional Disclosures

Among other things, the Cybersecurity Proposal would require an adviser to disclose cybersecurity risks and incidents to clients. An adviser would do so through new Item 20 of Form ADV Part 2A, which would describe the adviser's cybersecurity risks and how the adviser addresses them. Item 20 would also require advisers to describe any cybersecurity incidents within the previous two years that significantly disrupted the adviser's operations or led to data breaches harming the adviser or clients.

GDPR Notices

Like the CCPA, the GDPR requires covered advisers to provide a more detailed privacy notice than Regulation S-P. The required disclosures are similar to those required under Regulation S-P and the CCPA but vary sufficiently such that an adviser will usually need separate disclosures (either separate documents or separate sections within a single document) to comply with each law. For example, GDPR notices must include the adviser's legal basis for processing data, the contact information of the adviser's "data protection officer" in certain cases, the data retention period, and descriptions of a client's data

Continued on page 10

Continued from page 9

rights, which are more numerous than under Regulation S-P or the CCPA.

Written Policies and Procedures

Regulation S-P Requirements

In addition to disclosure requirements, Regulation S-P requires advisers to adopt written policies and procedures governing administrative, technical, and physical safeguards for the protection of customer data (a "**Data Plan**"), which should:

- Designate an employee or employees to coordinate the Data Plan;
- Identify reasonably foreseeable risks to the security of client data;
- Assess the sufficiency of safeguards in place to control risks;
- Address employee training and management; information systems; and detecting, preventing and responding to cyberattacks and data breaches;
- Design safeguards to control risks and regularly test the effectiveness of those safeguards;
- Evaluate and adjust the Data Plan based on testing results or changes to operations; and
- Provide for three levels of security for client data: (1) administrative security (written program, employee training, vendor oversight); (2) technical security (computer systems, networks, encryption); and (3) physical security (facilities, business continuity, disaster recovery).

Advisers Act Requirements

Advisers Act Rule 206(4)-7 requires advisers to implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and the rules thereunder. Because data privacy violations and data breaches could cause an adviser to violate its general duty of care as a fiduciary under the Advisers Act, advisers should address data privacy and cybersecurity in their policies and procedures as a matter of Advisers Act compliance independent of Regulation S-P obligations.

Regulation S-ID Requirements

Regulation S-ID requires advisers to implement a written identity theft prevention program, which must include policies and procedures to identify and detect evidence of client identity theft ("**red flags**"), as well as respond appropriately to red flags to prevent and mitigate identity theft.

Proposed New Standards

The Cybersecurity Proposal would require advisers to adopt written policies and procedures addressing the following elements:

- ***Cybersecurity risk assessment.*** Documentation of the adviser's cybersecurity risks, including conducting a prioritized risk inventory and identifying risks associated with the use of service providers.
- ***Access restrictions.*** Enumerated controls designed to minimize user-related risks and prevent the unauthorized access to information and systems.
- ***Data protection.*** Prescriptive network monitoring and data loss prevention procedures that are detailed in the proposed regulations.
- ***Cybersecurity threat and vulnerability management.*** Detection, mitigations, and remediation of cybersecurity threats and vulnerabilities.
- ***Cybersecurity incident response and recovery.*** Measures to respond to and recover from data breaches, including policies and procedures designed to ensure continued operations, the protection of data and data systems, external and internal data breach information-sharing and communications, and reporting of significant data breaches to the SEC.

The Cybersecurity Proposal would further require an annual review and written report assessing the adviser's cybersecurity policies and procedures, with results of control tests and incidents within the prior year.

GDPR Requirements

GDPR requires advisers covered by the law to adopt a Data Plan with many of the same elements as required by Regulation S-P. A Data Plan designed solely to comply with Regulation S-P requirements will largely comply with the GDPR, but additional components may need to be added to attain full compliance, such as provisions addressing data use limitations, data minimization, and data accuracy.

Service Provider Oversight

Under Regulation S-P, the SEC expects advisers to oversee service providers by selecting ones that maintain appropriate safeguards and requiring them by contract to maintain those safeguards. Moreover, Regulation S-P limits a service provider's reuse and redisclosure of NPI, regardless of whether the service provider is independently subject to Regulation S-P.

The CPRA will likewise mandate an adviser subject to the law to contractually require its service providers to assist it in complying with client requests to limit data transmitted from the adviser to the service provider. Advisers will also be required to conduct due diligence on service providers to effectively establish a defense against vicarious liability for a service provider's violation of the CPRA. As described above, this will not impact the processing of most client data but could impact the processing of data collected from an adviser's website or employee data.

The Cybersecurity Proposal would

Continued on page 11

Continued from page 10

also require advisers to supervise service providers that receive, maintain, or process client data and contractually require service providers to implement and maintain appropriate measures to protect client data.

Finally, the GDPR requires a covered adviser to contractually impose on service providers "appropriate technical and organizational measures" to protect client data and process client data only pursuant to the adviser's direct instructions. Because the EU deems the U.S. to have "inadequate" data privacy laws, transfers of client data from the EU to the U.S. must be governed by "standard contractual clauses" published by the European Commission to contractually protect the data.

Preparedness and Response

State Breach Notification Requirements

Every U.S. state has adopted a data breach notification law requiring covered entities, including advisers, to provide notice of a data breach to affected consumers, and in some cases, state regulators. Reportable breaches are not limited to the classic case of a hacker gaining access to an adviser's computer systems to steal client data. Typically, any unauthorized access of client data, even if inadvertent, is within scope of these laws. For example, a service provider inadvertently sending the wrong data file to another party could constitute unauthorized access.

However, an adviser need not report the unauthorized access of all types of client data. Usually, the only data subject to these laws consists of a client's name *in combination with* other data, often including Social Security number, driver's license number, account number, or account login credentials. Many states exempt encrypted data. Often a covered adviser will not need to disclose an unauthorized access of data to a client if there is not a high risk of harm to the client. Many states also impose numeric reporting thresholds, such that an adviser is only required to notify law enforcement or a state regulator if the data of more than x clients has been accessed. Timelines for reporting vary – usually between 30 and 60 days after discovery.

GDPR Notification Requirements

Article 33 of the GDPR requires an adviser subject to the law to notify applicable data protection regulators of a data breach within 72 hours of discovery when the breach has led to the destruction, loss, alteration, disclosure of, or access to client data. Article 34 requires the notification of affected clients only when a breach is likely to present "high risk" to the client. Thus, under GDPR, regulator notification is step one, and a severity threshold determines whether clients should be notified; in the U.S., client notification is step one, and a severity threshold determines whether regulators should be notified.

Proposed SEC Notification Requirements

The Cybersecurity Proposal would require advisers to file a report with the SEC on new Form ADV-C within 48 hours after a "significant" data breach and file an amendment after resolving such an incident. Form ADV-C would solicit, among other things, whether clients, law enforcement, or another regulator has been notified, the adviser's planned responsive action, whether any client data was accessed, and whether the breach is covered by insurance.

Conclusion

Protecting client information has become a significant concern for advisers with the evolution of the computer and social media age and the efficiencies which it has generated. These efficiencies have not come without a cost – particularly when it comes to protecting client information – as evidenced by recent breaches and corresponding actions of various federal and state regulatory authorities. Advisers should actively monitor developments in the area and seek to address their evolving obligations, given their fiduciary duties to their clients and the nature of the client asset being protected.

**Paul Miller is a partner and Casey Jennings is a counsel in the Washington, D.C., office of Seward & Kissel LLP. Paul can be reached at millerp@sewkis.com, and Casey can be reached at jennings@sewkis.com.*

The views and opinions expressed in this article are those of the author and do not necessarily reflect those of the IAA. This article is for general information purposes and is not intended to be and should not be taken as legal or other advice.