IAA Today
powered by SmartBrief

Compliance Corner
October 18, 2024

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

Casey J. Jennings

Paul M. Miller

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

Investment advisers understand their responsibility for safeguarding irreplaceable client assets such as family legacies, college tuition, and retirement savings. But the most important item an adviser stewards may well be a client's personal data, which, if misappropriated, can harm a client more than poor investment advice.

Client personal data is a target. Data breaches in 2023 hit an all-time high — the Identity Theft Resource Center identified over 3,000 data breaches affecting approximately 353 million individuals. Perhaps counterintuitively, the total number of victims dropped in 2023 from 2022, demonstrating a criminal focus on obtaining specific information to perpetrate identity-related fraud and scams rather than mass attacks.

Unsurprisingly, regulators have turned their attention to data issues and have recently taken the following actions:

- The SEC recently adopted amendments to Regulation S-P, applicable to SEC-registered advisers.
- The FTC recently amended its Standards for Safeguarding Customer Information Rule (the "Safeguards Rule"), applicable to investment advisers that are not registered with the SEC (private advisers).
- The SEC proposed the Cybersecurity Risk Management Rule in February 2022 (the "Cybersecurity Proposal"), which is expected to be adopted shortly.

In addition, the SEC staff issued a risk alert in April 2019 highlighting the SEC staff's concerns that firms were not adequately safeguarding client records and information under the safeguarding requirements of Regulation S-P.

In this article, we summarize the myriad regulatory obligations of registered and private advisers, which fall within three categories, discussed in turn below: (1) client disclosures; (2) written policies and procedures; and (3) preparedness, response, and notification.

Summary of 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. GLBA is implemented with respect to registered advisers through Regulation S-P and to private fund advisers through the FTC's Regulation P and Safeguards Rule (together, the "GLBA Data Regulations"). NPI is any data not otherwise publicly available that an adviser obtains in connection with a consumer financial product or service. The GLBA Data Regulations govern both data "privacy," referring to the permissible collection and use of NPI, and data "security," referring to the protection of NPI from unauthorized access or use.

Nearly all of an adviser's client data is NPI covered by the GLBA Data Regulations, 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 the GLBA Data Regulations. Regulation S-ID, which also applies to registered advisers, and the FTC's Red Flags Rule, which applies to private advisers, require advisers to adopt a written identity theft prevention program designed to identify relevant types of identity theft red flags and to detect and respond to them.

Additionally, advisers may be subject to the California 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 worldwide annual revenue of at least $25 million; (2) annually buy, sell, or share the personal information of 100,000 or more California residents or households; or (3) derive 50% or more of their revenue from selling California consumers' personal information. Although advisers are not per se exempt from the requirements of the CCPA, the CCPA does not apply its protections to data processed "pursuant to" 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 GLBA – is subject to the CCPA. The California Privacy Rights Act ("CPRA"), which amended the CCPA effective January 1, 2023, adds several new prescriptive requirements.

Many other states have recently adopted privacy laws, but those laws exempt financial institutions regulated under the GLBA, including advisers. Notably however, state data breach notification laws do apply to advisers.

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

Client Disclosures

Privacy Notices

The GLBA Data Regulations require advisers to provide clients a "clear and conspicuous" privacy notice in writing before collecting NPI that describes (1) the data collected by the adviser, (2) with whom the data is shared, and (3) how the adviser protects the data. Thereafter, advisers are required to transmit the privacy notice to their clients no less than annually, unless they meet an exemption.

Advisers are exempted from transmitting annual privacy notices if (1) they only share NPI with non-affiliated third parties pursuant to an exception that does not grant the client the right to opt-out of such sharing (such as sharing of NPI with a fund administrator, accountant, or payment processor), and (2) the adviser has not changed its privacy policies and practices that it disclosed in the last privacy notice provided to the client.

If an adviser shares NPI with non-affiliated third parties, it must provide the client the right to opt-out of such sharing unless an exception applies.

CCPA Notices
Like the GLBA Data Regulations, 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 required under the GLBA Data Regulations. Additionally, an adviser subject to the CCPA that sells or shares data must have a prominent "Do Not Sell or Share" button or link 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 Under the Advisers Act
Among other things, the Cybersecurity Proposal would require an adviser to disclose cybersecurity risks and incidents to clients. The 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 an adviser 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, GDPR requires covered advisers to provide a more detailed privacy notice than the GLBA Data Regulations. The required disclosures are similar to those required under the GLBA Data Regulations 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.

Written Policies and Procedures

Regulation S-P Requirements
In addition to disclosure requirements, Regulation S-P requires registered advisers to adopt comprehensive written policies and procedures governing administrative, technical, and physical safeguards for the protection of customer data (a "Data Plan"). The SEC's recent amendments to Regulation S-P further require advisers to:

- Adopt written policies and procedures for an incident response program to detect, respond to, and recover from a breach of client data;
- Notify affected individuals within 30 days after the adviser becomes aware that a data breach incident either occurred or is reasonably likely to have occurred;
- Enhance their oversight of service providers with respect to data processing; and
- Maintain written records documenting compliance with the amendments.

Advisers Act Requirements

Advisers Act Rule 206(4)-7 requires registered advisers to adopt and 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 registered 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. The FTC's Red Flags Rule imposes similar requirements on private advisers.

Proposed New Standards

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

- Cybersecurity risk assessment
- Access restrictions
- Data protection
- Cybersecurity threat and vulnerability management
- Cybersecurity incident response and recovery

GDPR Requirements

GDPR requires advisers covered by the law to adopt a Data Plan with many of the same elements as required by the GLBA Data Regulations. A Data Plan designed solely to comply with the GLBA Data Regulations 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

GLBA limits a service provider's reuse and redisclosure of NPI, regardless of whether the service provider is independently subject to the GLBA Data Regulations. Further, under the SEC's amendments to Regulation S-P, registered advisers must adopt written policies and procedures providing for the oversight of service providers, including through monitoring and due diligence. Specifically, the policies and procedures must be reasonably designed to ensure service providers (1) protect against unauthorized access to or use of client information; and (2)

provide notification to the adviser as soon as possible, but no later than 72 hours after becoming aware of a breach resulting in unauthorized access to a client information system maintained by the service provider. Private advisers have similar, though less prescriptive, requirements under FTC regulations.

The Cybersecurity Proposal would 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.

The CCPA likewise mandates 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.

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, Response and Notification

Regulation S-P Client Notification Requirements

The SEC's amendments to Regulation S-P require advisers that have experienced a data breach involving "sensitive customer information" to notify affected clients. Sensitive customer information consists of either: (1) information identified with an individual that, without any other information, could create a substantial risk of harm or inconvenience to that individual (such as a Social Security number, driver's license number, or alien registration number); or (2) combinations of identifying and authenticating information that could create a risk to an individual identified with the information (such as the individual's name and the individual's mother's maiden name).

Notice must be provided to affected individuals as "soon as is practicable" – and no later than 30 days – after discovering that a breach occurred or is reasonably likely to have occurred.

FTC Notification Requirements

Under the FTC's amended Safeguards Rule, advisers not registered with the SEC are required to notify the FTC as soon as possible, and no later than 30 days after discovery, of a "notification

event" involving the customer information of at least 500 individuals. A notification event is defined as the acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is unencrypted if the encryption key was accessed by an unauthorized person.

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.

State Client 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. Some 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 and reporting is usually required between 30 and 60 days after discovery.

Importantly, compliance with SEC or FTC reporting requirements does not necessarily satisfy state reporting requirements.

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 also be notified; in the U.S., client notification is step one, and a severity threshold often determines whether regulators should also be notified.

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.

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