January 5, 2022

Private Fund Cybersecurity Requirements Changing Significantly in 2022

Private funds that are excluded from the definition of "investment company" under sections 3(c)(1) or 3(c)(7) of the Investment Company Act of 1940 ("ICA") will face significantly stricter cybersecurity requirements under the FTC's revised Safeguards Rule, which comes into full effect as of December 9, 2022. The FTC's updated Safeguards Rule breaks new ground for the FTC by requiring specific security controls and accountability measures for consumer information expressly modeled on the New York Department of Financial Services' ("NY DFS") cybersecurity rule. For private fund entities covered by the Safeguards Rule, these changes will require prompt review, since many of the newly required controls will take time to implement. Among other things, the Safeguards Rule will now require multifactor authentication for any individual accessing information systems that store customer information (or compensating controls), encryption of all customer information both in transit and at rest (again with the option of alternative compensating controls), and updates to record retention procedures for customer information.

The revisions also dictate further specific governance controls by requiring reporting, at least annually, to a board of directors or senior officers about the private fund's security posture and the adoption of a formal incident response plan for those funds that maintain customer information regarding more than 5,000 consumers. Significantly, very few private funds would have more than 5,000 consumers; indeed, some may not have any "consumer" information for purposes of the Safeguards Rule, because "consumers" for purposes of this rule are natural persons investing primarily for personal, family, or household purposes, as opposed to business, commercial, or agricultural purposes.

The FTC's version of the Safeguards Rule applies to a broad range of "financial institutions" not subject to oversight by another functional regulator such as the SEC. These include mortgage brokers, nonbank lenders, investment advisers not registered with the SEC, and, critically for our asset management clients, entities such as many private funds that meet the criteria for exclusion from regulation under ICA §§ 3(c)(l) or 3(c)(7). Significantly, the FTC's Safeguards Rule offers little nuance as to complex investment arrangements and private fund structures, because it is intended to cover a very broad range of businesses, including "pay-day" lenders, check cashers, wire transferors, and collection agencies.

Other financial regulators, such as the SEC, have adopted their own versions of the Safeguards Rule. For SEC registrants, Reg. S-P is the primary rule with respect to the security of customer information. While the FTC's revisions will not apply to those rules, the FTC's views are likely to be influential in assessing whether the security programs adopted by organizations subject to SEC regulation, such as registered investment advisers and broker-dealers, are "appropriate" or "reasonable." Indeed, most of the items in the FTC's revisions to its Safeguards Rule are already part of a typical SEC Office of Compliance Inspections and Examinations ("OCIE") cybersecurity exam inquiry.

Background on the FTC's Safeguards Rule

The drafters of the Gramm-Leach-Bliley Act (GLBA), enacted in 1999, sought to establish new privacy and security standards for the protection of nonpublic personal information processed by financial institutions. Rather than impose specific security measures itself, the GLBA delegates authority to create such standards to financial regulators. These include, among others, the SEC, the Board of Governors of the Federal Reserve System, and the Board of Directors of the Federal Deposit Insurance Corporation. The FTC serves as a catch-all backstop of sorts, with authority to establish security standards for financial institutions subject to GLBA, but not subject to regulation by another functional regulator.

The FTC first promulgated its version of the Safeguards Rule in 2002, and the Rule became effective the following year. The FTC's Safeguards Rule, similar to versions promulgated by other regulators, requires financial institutions to develop and maintain a comprehensive written information security program that includes administrative, technical, and physical safeguards that are "appropriate" to the organization's size and complexity, the nature of its processing

activities, and the sensitivity of any customer data at issue. That requirement remains in place; however, the FTC's revisions now create additional, more granular security requirements that could necessitate significant compliance efforts. Although it is not surprising that regulators are refreshing nearly 20-year-old cybersecurity rules, it does merit attention that regulators seem to be approaching these new rules with more confidence that they can impose specific requirements, as opposed to requiring merely "appropriate" cybersecurity measures.[1]

FTC's Updates to Safeguards Rule

The FTC's recent updates make clear the existing expectation that there is a "a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[2]

The real impact for private funds comes in two changes to the Safeguards Rule: (1) significant new governance and accountability requirements and (2) new specific security measures. While many private funds may already have procedures in place to meet these requirements, it is critical to review not only a private fund's policies and procedures to confirm whether they need to be amended, but also the technical protections for the systems that house the data used by the private fund.

Governance and Accountability

Following the NY DFS model and SEC guidance, the Safeguards Rule first focuses on governance and accountability. Most financial regulators have recently emphasized the need not only to have appropriate policies and procedures in place, but also to ensure they are appropriately implemented, and the FTC's updates propose additional measures in line with that guidance. The requirement to appropriately implement information security policies and procedures may not seem especially onerous, but many organizations may not have that capability in house. As such, they may need to turn to outside service providers. The Safeguards Rule now requires appointment of a single "Qualified Individual" (who may be at the fund, an affiliate, or a service provider) to oversee and implement the organization's security program. Previously, an organization could appoint multiple employees to fill that role in coordination. This Qualified Individual must:

- **Assess risks:** periodically assess "reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information";[3]
- **Ensure technical safeguards:** design and implement safeguards to control these risks including the specific controls discussed below;
- **Monitor systems:** implement policies, procedures, and controls to monitor and log both the activity of authorized users and detect unauthorized users, which, in the context of a private fund, would likely indicate employees or contractors at the adviser who take care of the fund's data;
- **Train employees:** provide security awareness training and ensure that the personnel charged with protecting their systems are trained and have current knowledge of security threats;
- **Oversee service providers:** take "reasonable steps" to
    - select third parties that "are capable of maintaining appropriate safeguards,"
    - obtain contractual commitments that service providers will comply with such safeguards, and

- "periodically" assess the continued adequacy of the safeguards "based on the risk they present"; that is, having a policy that classifies vendors by risk and then subjects them to re-diligence on a regular basis. Commonly, such periodic review is implemented through annual assessments for high-risk vendors and assessments every two or three years for lower-risk vendors, although the regulations do not dictate any particular cadence;[4] and

- **Evaluate and adjust the program:** change the program when there are material changes to operations, business arrangements, or risks presented.

For organizations with more than 5,000 consumers, the Rule also now requires:

- a written risk assessment;

- continuous monitoring or periodic penetration testing and vulnerability assessments;

- development of a written incident response plan that clearly defines roles and responsibilities, addresses both external and internal communications and information sharing, and provides for the documentation and reporting of security events at least annually; and

- written reporting to a board of directors or similar body about the status of the information security program, or, if the organization does not have a board, reporting to a senior officer responsible for information security—which, for a private fund without officers or directors, may require a report to an officer of its general partner.[5]

As with the specific security requirements described below, these measures must be put in place by December 9, 2022, and should be considered best practices even for organizations with fewer than 5,000 consumers.

Specific Security Requirements

The Safeguards Rule also now requires covered financial institutions (including private funds) to put in place specific security measures, which could be done fund by fund, but could most effectively and efficiently be achieved through an overall data governance framework involving private funds, their investment adviser(s) and general partners. Although not formally or expressly required by the Safeguards Rule, in practice, this may result in a fund being part of its adviser's cybersecurity program. Such an approach would allow private funds to benefit from their advisers' existing programs, ensure alignment of the information security programs of private funds and their advisers, and reflect the realities of information sharing between these affiliated entities. As a practical matter, the program itself would normally cover affiliates only, but should require service providers (e.g., fund administrators) to comply substantively with the program when they are handling data from the fund family as a matter of vendor oversight.

Section 314.4 of the Safeguards Rule lists eight security requirements,[6] including several items that the SEC routinely requests in exams now and has strongly encouraged:[7]

1. Implementing and periodically reviewing access controls, including incorporating the principle of least privilege (i.e., giving the minimum level of access to an account necessary for an individual's job function);

2. Inventorying and classifying data and systems in a risk-based manner ("Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy");[8]

3. Encrypting all customer information, both at rest and in transit, or implementing compensating controls, approved by the Qualified Individual, if encryption is infeasible;

4. Adopting secure development practices for in-house applications;

5. Implementing multi-factor authentication for all access to information systems containing customer information, unless the Qualified Individual approves in writing the use of "reasonably equivalent or more secure access controls"—notably, this requirement applies not only to remote access but also to access from inside an organization's network firewalls (although multi-factor authentication inside of a firewall can be more transparent to the end user);

6. Maintaining data retention procedures requiring secure disposal of customer information *no later than two years* after the information is no longer needed for a business purpose or to comply with law or regulation, unless disposal is infeasible—retention policies must also be periodically reviewed and, as a practical matter, should be tied to the data inventory and classification process;

7. Adopting procedures for change management; and

8. Monitoring to detect unauthorized access to, use of, or tampering with customer information.

Although the regulation is formally effective January 10, 2022, the additional detailed measures must generally be adopted by December 9, 2022.

Conclusion

Organizations may need time to implement many of the measures described above. Fortunately, the FTC extended the time period for organizations to come into compliance to December 9, 2022 (the Rule as originally proposed allowed for only six months); however, even with that extended time period, organizations may struggle to meet all of the Rule's new requirements.

We recommend developing a comprehensive data governance strategy as soon as possible to ensure adequate time to prepare, normally as part of an overall data governance approach involving advisers, general partners, and private funds—and using in-house and external talent as needed.

This will start with the identification of data and systems, then the consideration of the risks to those data and systems, and finally the documentation of how controls mitigate those risks, including by disposing of sensitive data that is no longer needed. At the same time, it is crucial to ensure that training is adequate so that your employees and contractors are not the weakest link. Additionally, organizations will need to consider whether certain technical measures such as encryption are feasible for them, and if not, develop alternatives. Organizations must be prepared to justify these alternative measures as reasonably equivalent to the default technical standard should the FTC inquire.

Even for organizations that are not subject to the FTC's Safeguards Rule, the FTC's updates may provide additional guidance as to security measures that may be required by the FTC and by other federal financial services regulators. While most data security laws still rely on generalities such as "reasonable" or "appropriate" security, new laws and regulations are increasingly specifying measures required to satisfy these criteria. This trend is not new. The 2009 Massachusetts information security regulations at 201 CMR 17 broke ground here, and other recent examples include the New York SHIELD Act and the NY DFS Cybersecurity Regulations—which have now formed the basis of a model rule that has been adopted in more than a dozen states. Organizations should continue to monitor these developments as they review the adequacy of their security programs.

Please contact your regular Ropes & Gray LLP partner should you have questions or any of the U.S. data, privacy & cybersecurity partners, including Ed McNicholas, Edward.McNicholas@RopesGray.com.

1. The FTC Financial Privacy Rule also requires private funds to issue initial and annual privacy notices to natural person investors. The Safeguards Rule does not impact those requirements.
2. FTC Safeguards Rule § 314.3.
3. FTC Safeguards Rule § 314.4(a) & (b)(2).
4. FTC Safeguards Rule § 314.4(f).
5. The Safeguards Rule offers little guidance relevant to private funds on this reporting point. The preamble to the Safeguards Rule notes that the "provision is intended to ensure the governing body of the financial institution is engaged with and informed about the state of the financial institution's information security program. Likewise, this will create accountability for the Qualified Individual by requiring him or her to set forth the status of the information security program for the governing body." In light of these goals, it would seem that a written report from the Qualified Individual charged with responsibility for cybersecurity to an officer of the general partner would serve a similar purpose and help a private fund ensure its information security program is maintained appropriately and given the necessary resources.
6. FTC Safeguards Rule § 314.4(c)(1-8), effective December 9, 2022, but not subject to the §314.6 exemptions for 5,000 consumers.
7. *See* SEC OCIE, "Cybersecurity and Resiliency Observations" (Jan. 27, 2020) https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.
8. We note that SEC exams will already routinely request both "a copy of Adviser's policies and procedures relating to data classification [including] a list of the types of data classification, the risk level (e.g., low, medium, or high) associated with each data classification, the minimum controls required for each classification of data, and a description of how the factors and risks are considered when determining whether data fits within each classification" as well as "a copy of Adviser's inventory identifying where and how client NPI [non-public information] is maintained or stored, including a list of all third-party systems that are used to store client NPI."