Cyber Risk at Private Funds

A Talk with Ira Kustin and Sherrese Smith

Private funds hold large amounts of highly valuable data and assets. Advisors to private funds have personal, non-public information about investors, including income data and social security numbers. This information may be held by third party administrators, auditors, or other service providers. As important as the funds themselves are, this data is also very valuable; hackers can use such data to build large repositories and garner leads that will be of value to them. According, private funds are targets for cyber attacks. Some of the risks involved for private funds during a breach include:

- The theft of personal private information of investors, intellectual property and strategy theft, and more recently, the theft of real assets.
- Business disruption, like by the destruction or hiding of data through ransomware.
- Legal liability and contractual implications for gross negligence.
- Reputational harm following a breach or hack.

Private funds are governed by various state, federal, and international regulations, and these regulations often overlap with one another. The most complicated problem for private funds is often determining which regulations must apply to their policies. Once applicable regulations are determined, private funds should know that privacy policies can be encapsulated in one document that covers all relevant jurisdictions.

- U.S. federal regulations include:
    - The Investment Advisers Act of 1940 [1], which requires that entities compensated for advising must register to the SEC and abide by regulations intended to protect investors, after defining what constitutes an adviser. The Act has been amended a number of times, most recently in 2019.
    - Regulation S-P[2], which requires that broker-dealers, investment companies, and investment advisers adopt specific policies to protect customer records and information.
    - Regulation S-ID[3], the Identity Theft Red Flag Rules, are SEC and CFTC jointly adopted rules that require certain regulated entities to have programs to address and prevent identity theft.

[1] 15 U.S.C. S 80b-1 et seq., https://www.govinfo.gov/content/pkg/COMPS-1878/pdf/COMPS-1878.pdf.
[2] https://www.sec.gov/spotlight/regulation-s-p.htm.
[3] https://www.sec.gov/info/smallbus/secg/identity-theft-red-flag-secg.htm.

    - The Gramm Leach Bliley Act (GLBA)[4], which, in part, requires financial institutions to "explain their information sharing practices to their customers and to safeguard sensitive data."
- State laws of note include:
    - California Consumer Privacy Act (CCPA)[5] and Virginia's Consumer Data Protection Act (CDPA)[6]
        - The state laws offer some exceptions to their privacy and cybersecurity requirements. For example, in both California and Virginia, laws provide that private funds will be exempt to certain parts of the respective state laws where the GBLA applies. All data collected that is not exempt will be subject to state law.
- Application of other nation's laws
    - It is important that private funds understand their reach and how their reach influences the application of international laws. Namely, the GDPR is the most prominent privacy law. If a fund has or is receiving information about EU constituents and customers, that fund is subject to the General Data Protection Regulation[7].
- Funds should be aware that when using Cayman vehicles, bringing in non-U.S. investors, and bringing in tax-exempt U.S. investors, regulations for offshore funds like the Cayman Data Protection Law[8] may apply.

The U.S. Securities and Exchange Commission regulates securities markets and protects investors. Relevant to private funds, the SEC provides cybersecurity guidance and brings forth cybersecurity enforcement actions against such financial institutions. The SEC wields great power. Although some rules are vague, examiners of registered advisers expect certain specific policies that are required for the overall obligation to have policies and procedures under the Advisers Act.

Now, the SEC is focusing on cybersecurity and data protection in novel ways. Some areas of focus of the SEC can be clarified by. . .

- . . . Looking at recent guidance by the SEC. For example, Rule 206(4)-7[9] in part requires registered advisers to establish policies and procedures designed to prevent, detect, and correct violations of the advisers act.
- . . . Looking at Risk Alerts by exam staff. Risk Alerts are not necessarily rulemaking, but serve as unofficial guidance that serve as clear indicators of what is deemed as "reasonable," a standard that the SEC uses when assessing steps

[4] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.
[5] https://oag.ca.gov/privacy/ccpa.
[6] https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+HB2307.
[7] https://gdpr-info.eu/.
[8] https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Law_2017.pdf.
[9] https://www.sec.gov/rules/final/ia-2204.htm.

taken to prevent breaches. For example, a November 2020 Risk Alert[10] in part noted that registered advisers have an obligation to update policies and procedures annually in order to comply with the Advisers Act.

- . . . Looking at the annual Examination Priorities Report[11].

When a breach occurs, there are a couple of factors to consider:

- Obligation to report breaches
    - There is, in the most likely case, an obligation to report the breach. Private funds should contact their counsel in the event of a breach. Depending on the jurisdictions of the managers, fund entities, and investors, there may be requirements to notify regulators and investors about the breach.
- Enforcement
    - The penalties following a breach depend on the circumstances. Private funds that do all that is reasonable to prevent breaches are less likely to face SEC enforcement. Accordingly, more reckless or negligent advisers are more likely to face penalties.

Experts suggest that there are several new considerations that private funds should take into account that were less relevant in the past. These include:

- Updating policies and procedures; ensuring that policies and procedures are re-evaluated at least once per year.
- Paying closer attention to third parties and their privacy protocols; third parties may have privacy protocols that are not up-to-standard and put funds at increased risk of getting hacked. In forming contractual relationships with third parties and vendors, funds should anticipate and prepare for potential issues.

[10] https://www.sec.gov/files/Risk%20Alert%20IA%20Compliance%20Programs_0.pdf.
[11] https://www.sec.gov/files/2021-exam-priorities.pdf.