Professional Perspective

Regulatory Oversight of Privacy, Cybersecurity & Private Investment Funds

Margaret Dale, Kelly McMullon, Todd Ohlms, Hena Vora, and Jonathan Weiss, Proskauer

Bloomberg Law

Regulatory Oversight of Privacy, Cybersecurity & Private Investment Funds

Contributed by Margaret Dale, Kelly McMullon, Todd Ohlms, Hena Vora, and Jonathan Weiss, Proskauer

Privacy and cybersecurity issues continue to garner significant attention in the U.S. and abroad. Private investment funds registered with the SEC and their portfolio companies will likely see increased regulatory scrutiny relating to privacy and cybersecurity in the U.S., as will their counterparts in Europe.

This article focuses on recent developments in the U.S. and global enforcement and regulatory landscape—with a particular emphasis on developments in California, the EU, and the U.K. The enhanced regulatory focus on privacy and cybersecurity has been accelerated not only by recent changes in applicable regulatory frameworks, as discussed below, but also by changes in the nature of work in light of the pandemic. These developments are likely to spawn increased enforcement activity and litigation.

U.S. Enforcement & Regulatory Landscape

SEC 2021 Examination Priorities

The Securities and Exchange Commission's 2021 Examination Priorities, as in years past, identify the issues that will inform the agency's exams this year for cybersecurity. Given the impact of the pandemic on the way we work and communicate, the SEC expects that entities will have documented the changes to the way work is conducted and will have adjusted their risk management practices accordingly.

Highlights include:

- Challenges surrounding supervision of remote staff
- The need to maintain information security and operational resiliency around remote work
- A focus on material impacts of stresses to the market caused by the pandemic to portfolio companies owned by private investment funds, including increased cybersecurity risks

The move to remote work has increased risks related to, among other things, endpoint security, data loss, remote access, use of third-party communications systems, and vendor management. These areas will be a focus of the SEC's assessment, including whether firms have implemented reasonable controls to mitigate these and associated risks.

Cracking Down on Ransomware

There will likely be increased enforcement activity related to ransomware attacks, including the responses of the victims of such attacks. The frequency and severity of ransomware attacks has dramatically increased over the last decade, especially during the ongoing Covid-19 pandemic. In response, in October 2020, the Office of Foreign Assets Control (OFAC), a financial intelligence and enforcement agency of the U.S. Treasury Department, issued an advisory clarifying that any payment made to a sanctioned entity—even where the payment is made under the duress of a ransomware attack—would be a violation of federal regulations. Significantly, OFAC sanctions apply with strict liability, so the intent of the victim is no defense, nor is the victim's lack of knowledge that the payment is going to a sanctioned entity.

In its advisory, OFAC makes clear that it intends to enforce these regulations aggressively, even where a victim did not know it was paying a sanctioned party:

> OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

This raises a serious concern—where a criminal actor concealing its identity makes ransomware demands, the victim is unable to determine exactly who will receive a ransom payment, much less whether the party demanding payment is a

sanctioned entity. Ransomware attackers also force victims to make ransom payments through non-bank methods, often specific cryptocurrencies like Monero, making it difficult to identify the recipient of a payment by tracing wire transfer information or other traditional forms of transmitting funds.

Under these circumstances, a ransomware victim is highly unlikely to be able to determine whether a ransom payment is directed to a sanctioned entity. Victims of ransomware attacks should consult with experienced cybersecurity counsel to mitigate legal risks associated with potential responses to the attack.

Impact on Board Composition

Increased enforcement related to cybersecurity reaches far and wide, including to the board of directors of companies. Portfolio companies of private equity and venture capital firms are not immune, nor are their sponsor-appointed directors. The Federal Trade Commission (FTC) brought actions against a number of companies, including venture-backed companies, arguing that they failed to take reasonable steps to secure sensitive consumer information. The companies all reached settlements with the FTC, agreeing to incorporate comprehensive information security programs into their businesses.

These actions have the practical effect of holding boards responsible for ensuring that their companies implement sufficient cybersecurity protocols. Unfortunately, most board members lack formal education, training, and expertise in cybersecurity. These recent settlements may affect the composition of corporate boards, as companies search for directors who are knowledgeable about and have experience with cybersecurity best practices to help mitigate against the risk of unfavorable FTC treatment and cybersecurity exposure more generally.

Privacy in California

The California Consumer Privacy Act of 2018 (CCPA) became operative on Jan. 1, 2020, requiring qualifying businesses to enable consumers to know about and control the information collected about them. Notably, the CCPA does not require a business to have a physical address in California. Instead, the CCPA is triggered when the entity is "doing business" in California and meets one of three statutory thresholds: has annual gross revenues in excess of $25 million; annually buys, receives, sells, or shares the personal information of 50,000 or more California residents; or derives 50% or more of its annual revenues from selling residents' personal information.

In November 2020, California voters passed the California Privacy Rights Act of 2020 (CPRA) in an effort both to expand and strengthen the scope of the CCPA. Most of the changes effected by the CPRA—including modifications to the statutory thresholds mentioned above—will become operative on Jan. 1, 2023.

Because both the CCPA and CPRA define consumers and businesses broadly, private investment funds and their sponsors and managers may be considered "qualifying businesses," and information they collect and use about their employees, job applicants, investors, and prospective investors (including KYC information) residing in California could be subject to either or both of the acts.

However, there are some limited exemptions and exceptions that private investment funds and their sponsors and managers should evaluate including pre-emption and the applicability of Gramm-Leach-Bliley Act (GLBA) and the employee and business to business limited exceptions to the CCPA. This exemption analysis is fact specific and depends on how the personal information is collected, who it is collected from and what type of personal information it is.

The CPRA also expands the limited private right of action in the statute, allowing consumers to bring lawsuits, including class actions, against a company for data breaches involving additional categories of personal information. Notably, the CPRA adds email addresses in combination with a password or security question that would permit access to a customer's account to the list of actionable data types under the law in the event of a breach. Private investment funds registered with the SEC and their portfolio companies need to understand how the CCPA and CPRA apply to their operations and take necessary steps to ensure compliance.

Separate but related to the CCPA is the newly passed Virginia Consumer Data Protection Act (VCDPA), which goes into effect Jan. 1, 2023. Virginia is the second state to enact a comprehensive state privacy law, following California. The VCDPA is similar to the CCPA, and it will apply to entities doing business in Virginia.

The VCDPA will grant Virginia residents the right to know whether entities are processing their personal data, the rights to access, correct, and delete that data, and the right to opt-out of the processing of their data for purposes of targeted advertising, profiling, and sales to third parties. However, unlike the CCPA, the VCDPA does not have a private right of action and includes both entity-level and data specific exemptions, including financial institutions or data subject to the GLBA.

International Data Transfers under the GDPR

Outside of the U.S., the key law that grabbed much attention is the EU's General Data Protection Regulation (the GDPR) that has now been in force for three years. This omnibus law, applying to businesses and personal data across the board, has influenced the data privacy laws in a number of countries with GDPR-type laws being adopted in or proposed across the globe, including Brazil, India, and South Africa.

The GDPR applies to businesses that are established in the European Economic Area (EEA), as well as businesses that are not established in the EEA but that either offer goods or services to, or monitor the behavior of, data subjects—i.e., individuals—in the EEA. Following Brexit, the UK has in place an equivalent law that mirrors this extraterritorial reach.

There is renewed focus on international personal data transfers under the GDPR that require all businesses, including private investment funds, to look again at their international data flows to ensure that any transfers of personal data outside of the EEA provide an essentially equivalent level of protection.

This is as a result of a CJEU (Court of Justice of the European Union) judgment, C-311/18 (Schrems II) in July 2020, as well as the European Data Protection Board's (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the Recommendations) in June 2021 and the Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (the EEG Recommendations), in November 2020.

The decision in Schrems II meant that data transfers that were being made under the EU-US Privacy Shield were no longer lawful, and an alternative lawful basis needed to be relied upon. However, despite the Standard Contractual Clauses—SCCs, the most common method used to transfer personal data internationally—not being struck down by the CJEU, the CJEU held that additional analysis must now be carried out in order to determine if so called "supplementary measures" also need to be put into place to ensure an essentially equivalent level of protection. The decision also impacts those businesses relying upon the binding corporate rules—BCRs, another transfer tool that can be relied upon to transfer personal data between group companies.

The Recommendations set out certain steps that every business that transfers internationally must consider with respect to relevant international data transfers. Certain of those steps place a great burden on businesses—particularly small and medium-sized enterprises—and will likely require significant consideration and resource to be dedicated to them.

This is because they will need to, for example, make an appropriate assessment of the third country's law and practice, and then assess whether any additional technical, contractual, and organizational measures are needed to be implemented in order to protect the personal data being transferred. If these steps are not carried out, there is a risk the business will be subject to litigation or other enforcement action.

In addition, businesses, including private investment funds, will need to consider the SCCs themselves, given that the EU Commission also published new SCCs in June. Businesses now have until December 27, 2022 to ensure that the new SCCs are in place in relevant circumstances. Depending on personal data flows and transfers, this could be a time-consuming process. The UK's data protection regulator, the ICO, has also published its own international data transfer agreement (to replace the SCCs) and associated guidance for consultation.

Conclusion

Recent changes and developments in privacy laws in the U.S. and the EEA will sharpen the focus of regulators on the privacy and cybersecurity efforts of private funds and their portfolio companies. These developments, combined with changes in the nature of work caused by the pandemic, are likely to lead to an increase in enforcement activity and related litigation in the coming months.

Key takeaways related to private investment funds include:

- The need to implement reasonable controls around remote working conditions
- When faced with ransomware demands, consider regulatory risks of making payments to unknown entities
- The need for proactive Board oversight relating to cybersecurity risks and preparedness, especially where there are sponsor-appointed directors on a private investment fund's portfolio company's board
- Understanding the scope and reach of U.S. and international privacy regulations, and in this context understanding the data flows and data transfers within the private investment fund