ROPES & GRAY

ALERT

Privacy & Data Security

May 11, 2016

Key Data Privacy and Security Concerns for Investment Firms

I. Introduction

Privacy and data security concerns are among the most critical issues facing investment funds, advisors and managers (collectively, "investment firms"). This article outlines the privacy and data security challenges confronting investment firms, including the increased focus on the privacy and security of sensitive information by state, federal, and foreign authorities. With daily attacks by hackers on corporate networks and the looming threat of government enforcement actions and civil litigation, investment firms are wise to develop and implement effective strategies to protect their organizations and the portfolio companies they manage from privacy and security threats.

Attorneys

Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Rohan Massey
Seth C. Harrington
David M. McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
Deborah Gersh
Laura G. Hoey
David T. Cohen
Jennifer L. Romig
Sunil Shenoi

II. Privacy and Data Security Challenges

Investment firms have always been highly attractive targets for cyber criminals because of the extremely sensitive information they possess. While the security of personal and financial information has garnered most of the attention over the last ten years, investment firms also should focus their attention on the protection of non-public information of potential transactions, as failure to secure such information could place such transactions in jeopardy. A security breach resulting in the disclosure of such sensitive information could cost the investment firm hundreds of millions of dollars in remediation and litigation costs, not to mention the reputational harm of such a breach.

Not only should investment firms secure their own networks and information, it is important that they consider and address the privacy and data security practices of the portfolio companies they manage because a privacy or security incident could undermine a firm's investment in a portfolio company. For similar reasons, investment firms should review the privacy and data security practices of third-parties with which portfolio companies contract to provide services. Managing privacy and data security risk within a portfolio is an especially challenging task, given that an investment firm's portfolio likely includes a broad range of industries, varying types of information that must be secured, and a host of third parties interacting with those portfolio companies.

III. Complex Regulatory Environment

A. Privacy and Data Security Regulators

The active regulatory environment and the various agencies involved in the regulation of consumer and investor data creates additional complexity in complying with the myriad of privacy and data security rules and regulations. In the United States, several federal agencies, including the Federal Trade Commission, Federal Communications Commission and Consumer Financial Protection Bureau, have claimed authority to regulate privacy and data security. Determining which agency is likely to claim jurisdiction (and sometimes there is more than one) will depend on the business sector of the company, the activities in which the company is engaged, or the underlying data at issue. Several state Attorneys General have also sought to regulate corporate privacy and data security practices, with a handful of states often taking a leadership role in multi-state investigations. Investment firms can further be subject to foreign privacy and data security obligations, so they must closely examine key privacy and data security developments in countries in which they operate and/or invest, such as the European Union's recent General Data Protection Regulation (adopted by the EU Council and Parliament in April 2016).

Additionally, the U.S. Securities and Exchange Commission has increasingly focused on cybersecurity risks facing investment firms. In April 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced a series of examinations to identify data security risks in the securities industry. Following completion of these examinations, in February and April 2015, OCIE provided guidance to investment firms regarding three broad categories of cybersecurity protections they should implement: 1) conduct periodic risk assessments regarding cybersecurity practices, 2) develop a cybersecurity strategy to prevent, detect, and respond to cybersecurity threats, and 3) implement that strategy through policies, procedures, and training. On September 15, 2015, OCIE announced a second round of examinations that would focus on six key areas: 1) governance and risk assessment, 2) access rights and controls, 3) data loss prevention, 4) vendor management, 5) training, and 6) incident response.

The SEC's identification of these six areas, combined with OCIE's April 2015 guidance, provides a framework for the type of cybersecurity program that the SEC expects investment firms to adopt. Further, the SEC's public pronouncements on cybersecurity indicate that failure to meet these expectations can result in an enforcement action. Indeed, on September 22, 2015, only one week after its notice of a second round of cybersecurity examinations, the SEC announced its first settlement of an enforcement action against an investment adviser arising from a cybersecurity breach. In that case, R.T. Jones Capital Equities Management allegedly failed to establish cybersecurity policies and procedures prior to a breach of the personally identifiable information of approximately 100,000 individuals that was stored on a third-party-hosted web server. Even though none of R.T. Jones' clients were alleged to have been harmed as a result of the intrusion, R.T. Jones agreed to pay a $75,000 penalty as part of the settlement.

B. HIPAA Enforcement

While many of the regulators described above could attempt to regulate both an investment firm and its portfolio companies, firms that invest in the health care industry must also be aware of their obligations relating to the protection of healthcare data.

The Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and their implementing regulations (collectively, "HIPAA") requires the protection of individual health information and applies to entities known as "covered entities" and "business associates." An investment firm's portfolio companies, such as health care providers or data analysis and storage organizations, may be covered entities or business associates, and as a result would be subject to HIPAA.

The Department of Health and Human Services Office for Civil Rights ("OCR") is responsible for enforcing HIPAA. In general, OCR enforces HIPAA by investigating complaints and reported breaches, although under its audit program it additionally conducts periodic, proactive audits of covered entities and business associates. OCR may impose civil monetary penalties on covered entities and business associates that range from $100 to $50,000 per violation (with an annual maximum fine per violation of $1.5 million), with aggregate penalties trending higher in recent years.

Other entities may also be involved in HIPAA enforcement activities. The Department of Justice, for example, may investigate complaints alleging a violation of a criminal provision of HIPAA. Additionally, state Attorneys General have the authority to bring civil actions for HIPAA violations on behalf of state residents. Finally, the FTC has worked with OCR on joint enforcement actions related to privacy violations. For example, in 2010, FTC and OCR pursued joint enforcement under HIPAA and the FTC Act against Rite Aid, at the time publicly traded but partly owned by a private investment firm, for Rite Aid's alleged failure to safeguard the privacy of its consumers when disposing of identifying information on pill bottles labels and other information. Rite Aid paid a $1 million fine and agreed to a 3-year corrective action plan with HHS, and is subject to an FTC consent order for 20 years.

IV. Mitigating Cybersecurity Risks

Based on the risks and complex regulatory obligations faced by private investment firms, it is important that such firms develop an effective privacy and data security program. Set forth below are some of the proactive steps an

investment firm can take to mitigate cybersecurity risks, although all strategies should be carefully tailored to address the risks applicable to a particular entity.

A. Pre-Acquisition Diligence

Investment firms should conduct appropriate due diligence on potential investments or acquisition targets to minimize risk to the target and to the firm post-closing. Representations and warranties in the transaction documents can help limit risk but diligence should be undertaken to understand how a potential target collects, uses, stores, discloses, transfers, and disposes of data in its business operations. Prior to signing, investment firms should also develop post-closing remediation plans and evaluate how such plans impact the valuation model for the investment.

B. Policies and Procedures

Investment firms should develop policies and procedures to prevent, detect, and respond to security threats. Such policies and procedures should clearly document privacy and security expectations at the enterprise level and address the types of technical safeguards that firms should employ. Investment firms should also have a written incident response plan that clearly defines the roles and responsibilities for managing the incident, as coordination between various internal stakeholders is critical to a successful response. The response plan should account for the retention of legal, technology and public relations experts and the plan should be a living document. In other words, the plan should be tested, adjusted to account for the testing experience, and periodically tested again ideally involving the retained specialists so that when an incident happens, the entire team is ready to work together in a productive, efficient manner.

C. Training and Assessments

Investment firms should also develop and implement training programs for officers and employees regarding privacy and security obligations, security threats, and responses to such threats. Such training should cover the monitoring of compliance with the firm's policies and procedures regarding security. As part of a firm's monitoring efforts, an investment firm should also conduct periodic assessments regarding its technology infrastructure, internal and external cybersecurity threats, its governance structure for managing cybersecurity risks, and common networks shared with third parties. These assessments should be conducted under privilege wherever possible and appropriate.

D. Vendor Management

Given the impact that third-party privacy and data security practices can have on an investment firm and its portfolio companies, investment firms should establish a robust vendor management program. Such programs typically have three components: 1) a process to select and retain third-party providers that are capable of maintaining the security of the company's network and data, 2) standard contractual clauses to implement security controls that are appropriate to the services being provided, and 3) ongoing monitoring of the relationship over time to ensure that the vendor continues to have in place appropriate controls designed to protect the client's systems and data.

E. HIPAA Compliance Programs

Entities subject to HIPAA should ensure that their HIPAA compliance programs are comprehensive and up to date. In particular, entities subject to HIPAA are required to undertake a periodic "risk analysis" in order to assess risks and vulnerabilities to patient information. This analysis has become a focal point of OCR HIPAA enforcement and is often among the first documents requested by OCR during a HIPAA audit or investigation. Entities subject to HIPAA should also ensure the sufficiency of their policies, procedures, practices and training. Finally, entities subject to HIPAA should ensure that business associate agreements are in place as required; this has also become an OCR focal point in recent years.

* * *

Ropes & Gray LLP's global privacy and data security practice has assisted leading companies in developing and implementing tailored cybersecurity and HIPAA compliance programs, including policies, training, assessments, and

diligence processes. In addition, Ropes & Gray has helped organizations in a wide range of industries investigate data breaches and resolve government and consumer litigation stemming from data breaches. Recently, Ropes & Gray was named "Privacy Group of the Year" by a leading legal publication. For more information regarding data privacy and security, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Rohan Massey, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, Deborah Gersh, Laura Hoey, David Cohen, Jennifer Romig, Sunil Shenoi or another member of Ropes & Gray's leading privacy & data security team.