Cybersecurity: A Legal and Regulatory Primer for Private Equity Managers

John Araneo
Managing Director & General Counsel,
Align Communications, Inc.

Introduction: Regulatory Landscape and Increased Scrutiny on Private Equity

The Private Equity world has already endured tectonic shifts in the regulatory landscape in which it resides. Prior to the financial crisis of 2008, Private Equity funds (PE Funds) and the managers that oversee them (PE Managers) were largely unsupervised and unregulated. However, since July 21, 2010, with the enactment of Dodd-Frank Wall Street Reform and Consumer Protection Act, the regulatory expectations of both PE Funds and PE Managers have consistently increased in both scope and intensity. The current compliance requirements placed squarely on PE Managers and other fiduciaries and advisers to PE Funds have never been greater than as they stand today. For example, the Securities and Exchange Commission (the Commission), has previously charged forward with a series of enforcement actions against PE Funds, all based on a variety of conflicts of interest. The net takeaway from that regulatory initiative was the Commission's expression of its belief that these conflicts are inherent to the nature of the Private Equity model, which by design benefits from generally low expectations of operational transparency, historically loose expense allocation practices, illiquid and hard-to-value assets, and—when compared to its hedge fund siblings—a typically prolonged investment period. It seems now, as of the time of this writing, the regulatory hot issue has moved on to Cybersecurity.

The Rise of Cybersecurity As a Regulatory Priority

The Cybersecurity phenomenon has upended the risk management paradigm in both the investment management industry and the broader financial services sector. Indeed, Jay Clayton, the current Chairman of the Commission has characterized Cybersecurity as a substantial and systematic risk to the financial markets and moreover, prior Chairs of the Commission have noted that Cybersecurity is the biggest threat facing the global financial system. Additionally, certain recent developments within the regulatory landscape, including: (i) sizable investments made by the Commission to augment its technological and operational capabilities, allowing it to better identify and understand actual Cybersecurity failures in practice; (ii) the creation of a "Cyber Unit" to work hand-in-hand with the existing examination (OCIE) unit, as a separate enforcement division that is empowered to bring Cybersecurity enforcement actions; (iii) the continued Cybersecurity sweeps being launched by the Commission; and (iv) the fact that Cybersecurity continues to remain a top regulatory priority for the last five years, all portend that Cybersecurity compliance is a top line risk management issue for PE Managers that is not going away and one that is continually evolving. Thus, as PE Funds and PE Managers continue to remain prime regulatory targets and with Cybersecurity being one of the top risk items on the regulators' watch list, it is incumbent on every PE Manager to understand its legal, compliance, and fiduciary obligations in connection with Cybersecurity.

Cybersecurity Preparedness: An Emerging Legal Standard

The body of jurisprudence surrounding Cybersecurity is, like the phenomenon itself, still somewhat nascent. Federal and state laws that address Cybersecurity lack consonance and largely coexist inharmoniously, as a crazy quilt of competing federal, state, local and industry laws, regulations and rules, rife with friction points and inconsistencies. So too is the case with our international neighbors and the rest of the world. As it stands today, the controlling legal standards relating to

PE Funds and PE Managers have emerged from the usual channels, to wit, statutes and regulations on the one hand and regulatory pronouncements and enforcement actions by the Commission, on the other.

Statutory Authority and Applicable Regulations – How the Commission Asserted Jurisdiction Over Your Data Network

The Investment Advisers Act of 1940 (The Advisers Act)

The Advisers Act has no express provision that directly or explicitly addresses Cybersecurity. However, in light of the frequency, sophistication, and sheer volume of modern-day Cybersecurity attacks and breaches, a minimum standard of care relating to protecting client data, proprietary and/or confidential information, and other intellectual assets has been established and tested. Put another way, any PE Manager that fails to have reasonable Cybersecurity controls in place would likely run afoul of the fiduciary standards of the Advisers Act, especially since a negligence standard has been shown to impart liability thereunder. See SEC v. Capital Gains Research Bureau, 375 U.S. 180 (1963) (holding that a violation of § 206(2) may rest on a finding of simple negligence); SEC v. Steadman, 967 F.2d 636, 637 (D.C. Cir. 1992) (noting that a violation of § 206(4) does not require that the defendant acted with scienter). In fact, the Commission has suggested that under certain circumstances, a Cybersecurity breach could violate even the antifraud provisions of the Advisers Act. See September 15, 2015, SEC OCIE Risk Alert: 2015 Cybersecurity Examination Initiative, discussed below.

Regulation S-P – The Safeguards Rule

Regulation S-P was enacted by the Commission in response to the privacy provisions of the Gramm-Leach-Bliley Act, (15 U.S.C.§ 6801 (2006)), which required the Commission and certain other federal agencies to adopt privacy rules imposing requirements and restrictions on certain financial institutions' ability to disclose nonpublic personal information about its customers to non-affiliated third parties. Specifically, Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) requires firms to adopt written policies and procedures reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Regulation S-ID – The Identity Theft Red Flags Rules

On April 10, 2013, the Commission adopted Regulation S-ID (SEC Release No. 34-69359 (April 10, 2013), (78 FR 23638 (April 19, 2013)), requiring certain market participants, including PE Managers, to develop and implement a written program to "detect, prevent, and mitigate identity theft" in connection with client account information. Although it's possible for a PE Manager to fall within the purview of Regulation S-ID, it's highly unlikely that either PE Fund investors or the limited partnership (or other) interests they hold will meet Regulation S-ID's definitions of a consumer and a transaction account, respectively. As a practical matter however, this caveat is, in the end, moot, as the most meaningful obligations under Regulation S-ID (i.e., to detect, prevent, and mitigate identity theft) are arguably subsumed by the many requirements of Regulation S-P and the Commission's pertinent enforcement actions.

Regulatory Pronouncements

Building on these statutory and regulatory foundations, the Commission has recently made numerous expressions regarding its focus on Cybersecurity and the risks it poses to the markets and investors, as follows:

January 30, 2014 – SEC Investment Advisor 2014 Compliance Outreach Program

At this outreach program, the Commission highlighted Cybersecurity as one of several regulatory priorities and encouraged registrants to ensure that Cybersecurity policies are current and regularly assessed for their adequacy against this evolving risk.

March 26, 2014 – SEC Cybersecurity Roundtable

The roundtable provided a forum in which the Commission could become better informed about Cybersecurity by way of an open dialogue with registrants, market participants, fellow agencies, and representatives from the private sector who understand Cybersecurity risks and how best to combat those risks. It also provided the attendees (or their proxies) an opportunity to engage the Commission on these developing issues. Major themes included (1) the need for a public-private partnership through which technical information could be shared and to induce mutual assistance, (2) the value of a written Cybersecurity program and an incident response plan, and (3) the level of board engagement.

April 15, 2014 – SEC OCIE Risk Alert – Cybersecurity Initiative

The Commission's Office of Compliance Inspections and Examinations (OCIE) announced its Cybersecurity Initiative, a regulatory exercise encompassing over 100 registered broker-dealers and investment advisers. The Commission's focal points for these planned Cybersecurity sweeps included governance, identification and assessment of Cybersecurity risks, protection of networks and information, remote customer access, fund transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain Cybersecurity threats. This risk alert also included a sample list of document requests (the 2014 Risk Alert Appendix) which categorized and enumerated certain items the Commission may seek in connection with a Cybersecurity sweep or examination. The 2014 Risk Alert Appendix is particularly significant in that it included inquiries about policies, practices, and controls that go beyond the personally identifiable information (PII) of an investment adviser's clients, signaling for the first time that the Commission also expects PE Managers to protect certain valuable proprietary information, including information about their trading strategies, employees, investment programs, and other intellectual assets of the firm other than their clients' PII.

February 3, 2015 – SEC OCIE Risk Alert – Cybersecurity Examination Sweep Summary

The summary outlined the findings of the 57 registered broker-dealers and the 49 registered investment advisers that were subject to the sweep. The summary provided certain industry baseline facts surrounding Cybersecurity preparedness and revealed, among other things, that most advisers had adopted Cybersecurity policies and procedures, but less than half of them actually followed through with the required periodic assessments, even though a very high majority of the examinees reported suffering cyberattacks. The summary went on to report that fewer than one-quarter of the examined investment advisers had considered Cybersecurity as it relates to third-party vendors and also addressed other Cybersecurity trends and considerations for investment advisers, including identifying best practices through information-sharing networks, designating a Chief Information Security Officer, managing vendor relationships, and obtaining Cybersecurity insurance.

April 2015 – SEC Division of Investment Management Guidance Update

The Commission's Division of Investment Management (the Division) provided this guidance update as a further clarification on the Commission's prior directives surrounding Cybersecurity compliance. Essentially, the Division suggested that investment advisers implement several Cybersecurity controls and procedures. First, investment advisers should conduct periodic assessments in several areas, including (1) the information stored and used, including the technology systems used in connection therewith, (2) Cybersecurity threats, both internal and external, (3) existing security controls, (4) the impact of a Cybersecurity attack, and (5) the effectiveness of the current governance framework in place. Second, the Division addressed creating a strategy to prevent, detect, and respond to these threats and, in doing so, to consider such things as user credentials, authentication methods, encryption, data backup techniques, and an incident response plan. Finally, the Division recommended these controls to be implemented via policies and procedures that are customized to the scope and nature of each investment adviser and its business.

September 15, 2015 – SEC OCIE Risk Alert – 2015 Cybersecurity Examination Initiative

Building on the cumulative materials that preceded it, as well as the results of the Cybersecurity sweeps in 2015 and the previous years, this risk alert articulated a clear examination focus not on the mere existence of a Cybersecurity compliance program but rather how effectively such Cybersecurity Program has been implemented, and the actual, demonstrable integration of the controls espoused therein. This risk alert also provided much needed clarity on the largely principals-based guidance materials issued up to that point by identifying certain functional categories that should be included in any Cybersecurity program. Such categories include (1) governance and risk assessments, (2) access rights and controls, (3) data loss prevention, (4) vendor management, (5) training, and (6) incident response. Furthermore, the risk alert provided an updated appendix of document requests that OCIE may review in conducting examinations of investment advisers, which follow these categorical lines. OCIE also makes clear in this risk alert that a breach, in of itself, would not necessarily impart liability, by stating that it "recognizes that it is not possible for a fund or adviser to anticipate and prevent every cyber attack." Finally, footnote nine of this risk alert provides interesting commentary to the effect that any breach caused by insiders, such as fund or advisory personnel, could lead by fraudulent conduct to an investment adviser, in violation of the antifraud provision of the

Advisers Act.

May 17, 2017, OCIE Risk Alert – Ransomware

Following the largest ransomware cyber attack in history, OCIE released yet another risk alert, this time focusing on ransomware as a specific Cybersecurity threat. Illustrative of the Commission's increased intelligence and awareness on specific Cybersecurity threats, this risk alert provided a detailed explanation of how these attacks have actually infiltrated target firms in both the technical and technological context. This risk alert also reemphasized the need for firms to customize their Cybersecurity programs to their size, sophistication, and resources and made specific mention of basic Cybersecurity considerations for smaller firms.

January 2019, OCIE Risk Alert – Electronic Messaging

In response to the already-pervasive and growing use of both: (i) social media, texting and other types of electronic messaging applications; and (ii) the deployment of mobile and personally-owned devices, the SEC conducted a limited-scope examination initiative of investment advisers to gain an understanding of the various forms of electronic messaging used by advisers and their personnel, the risks of such use, and the challenges presented in complying with their obligations under Rule 204-2 (the "Books and Records Rule") and Rule 206(4)-7 (the "Compliance Rule") of the Advisers Act, respectively. The SEC identified several practices that "may assist" all investment advisers, including PE Managers, in meeting their record retention obligations under the Books and Records Rule as well as the concomitant design and integration of policies and procedures required under the Compliance Rule. These suggested practices contemplate: (i) drafting certain policies and procedures designed to provide control over, transparency to, and the ability to monitor, such communications; (ii) using Employee Training and Attestations, (iii) implementing various supervisory review tactics, regarding employee social media and online activities; and (iv) deploying adequate mobile device controls.

April 16, 2019, OCIE Risk Alert – Regulation S-P Privacy Notices and Safeguard Policies

Demonstrative of the importance of the Safeguards Rule to the Commission's evolving policy on Cybersecurity, this risk alert focuses on compliance with two of the rule's critical components, to wit, privacy policies and the duty to protect client information. Here, the Commission noted the most common deficiencies in this regard and (perhaps by default), provided certain best practices. The deficiencies noted by the Commission include failures to provide accurate privacy and opt-out notices, lack of accurate policies and specific procedures and blatant failures to implement these policies through the actual integration of reasonably-designed, achievable Cybersecurity control practices.

May 31, 2019, OCIE Risk Alert – Safeguarding Customer Records and Information in Network Storage

Coincident with the growing use of public and other cloud environments by investment advisers, the Commission identified numerous concerns regarding the use of myriad network storage solutions for electronic client data. These concerns included: (i) misconfigured network storage solutions; (ii) inadequate vendor oversight; (iii) insufficient data classification policies; and (iv) deficient configuration management programs. As investment advisers and particularly PE Managers continue to explore the use of could-based environments for their workflows and data storage needs, there must be a corresponding effort by such advisers to understand what and how data is being handled by these third-party vendors. In this risk alert, the Commission hinted towards its expectation that Cybersecurity risk management presumes a "shared responsibility" construct between each firm and its third-party cloud service providers. As a result, the expected levels of procedural accuracy and technological granularity of policies regarding the use of cloud solutions and services have reached a new high-water mark.

Enforcement Actions – The Commission's Application of the Laws, Regulations, and Interpretive Guidance Materials

In re: R.T. Jones Capital Equities Management, Inc.

On September 22, 2015, the Commission's Enforcement Division announced a settlement with R.T. Jones Capital Equities Management, Inc. (R.T. Jones) in connection with an enforcement proceeding surrounding R.T. Jones' failure to establish reasonable Cybersecurity policies and procedures. Essentially, R.T. Jones stored the PII of more than 100,000 individuals on its third-party hosted servers between September 2009 and July 2013. These servers were infiltrated by a cyber-attack emanating from China.

Significantly, the Commission noted that R.T. Jones failed to conduct periodic risk assessments, failed to employ a firewall to protect the client information, and failed to encrypt the client information on the server or

establish procedures for responding to a Cybersecurity incident. However, the Commission also noted that once it learned of the breach, R.T. Jones (1) promptly engaged more than one Cybersecurity consulting firm to take remedial action, (2) provided notice to all parties that their PII was compromised, and (3) offered free identity theft monitoring to such parties. Significantly, the Commission also found no evidence that such PII was actually ever stolen or even affected.

Nonetheless, the Commission took the position that R.T. Jones had violated the law by failing to adopt policies and procedures reasonably designed to protect against threats to the security of its client and third-party information, pursuant to Regulation S-P. Ultimately, the Commission censured R.T. Jones, ordered it to cease and desist from further violations, and to pay a $75,000 fine. Thus, the Commission has made it clear that even in the absence of an actual attack or a security breach, the failure of an investment adviser to design and implement a Cybersecurity Program is actionable.

In re: Morgan Stanley Smith Barney LLC

On June 8, 2016, the Commission's Enforcement Division announced charges against Morgan Stanley Smith Barney LLC (MSSB) for failing to adopt written policies and procedures reasonably designed to protect customer records and information, pursuant to Regulation S-P. The Commission found that MSSB allowed its employees to access its customer information through certain internal web applications or portals. Galen Marsh (Marsh), an individual who worked for MSSB in various capacities from 2008 until 2014, determined that, sometime in 2011, he was able to access these customer records and, without authorization, accessed information regarding more than 730,000 customers and transferred these data to his personal server over the internet.

The Commission of course found that MSSB had numerous systematic failures with regard to its obligations under Regulation S-P, including that MSSB (1) did not have effective authorization modules over these portals for a period exceeding ten (10) years, (2) did not audit or test the relevant authorization modules, and (3) failed to monitor or analyze any employee access or use of the portals. However, although it was clear that MSSB failed to adopt polices and procedures reasonably designed to protect customer records and information enterprise-wide, the Commission commended MSSB's exemplary response efforts, which included self-reporting the incident to the Commission, discovering the breach by way of its own efforts and vigilance, terminating the offending employee, and swiftly engaging both an independent consulting firm and a law firm to advise it on how to handle the incident, both internally and externally. In the end, MSSB agreed to pay a fine of $1,000,000.

The Morgan Stanley enforcement action remains a significant regulatory development regarding Cybersecurity relating to investment advisers, including PE Managers, for several reasons: (i) the amount of penalty itself demonstrates the Commission's perceived gravamen of Cybersecurity failures; (ii) the respondent, which is a large, sophisticated, and leading financial firm illustrates the Commission's willingness to pursue Cybersecurity violations against any adviser, large or small; and (iii) it demonstrates that liability—and a significant fine—may be imputed to an investment adviser even in the absence of any actual investor harm or damages, especially if the failures are systematic and enterprise-wide.

In re: Voya Financial Advisors, Inc.

On September 26, 2018, the Commission's Enforcement Division announced a settlement of certain charges against Voya Financial Advisors, Inc. (Voya) for certain Cybersecurity failures that violated both the Safeguards Rule and the Identity Theft Red Flags Rule. Notably, this is the Commission's first Enforcement Action regarding the Identity Theft Red Flags Rule since it began enforcing this rule in 2011.

By way of background, Voya is a dually registered as a broker-dealer and investment adviser, with approximately 13 million customers and approximately $11 billion in assets under its management with over 1,000 employees, as well as 3,800 other associated persons, including contractor representatives, across 1,200 locations. The firm's employees and its outside contractors both had access to its clients' PII. The Cybersecurity failures cited in this action surround a rather cunning hack, wherein the hackers called the firm's technical support line, impersonating certain contractors and requesting a reset of their credentials which instantly gave the hackers access to this PII. In this case, similar to the MSSB matter discussed above, the Commission found no fraudulent activity or direct investor harm, however the Commission did take issue with the fact that although Voya did have numerous policies that addressed Cybersecurity, they were not reasonably designed to the specific risks Voya faced nor were they reasonably integrated into its day-to-day operations.

More specifically, the Commission found that since these contractor accounts had previously been the target of prior hacks and were a known

vulnerability, Voya was derelict in its fiduciary duties to: (i) create policies that were reasonably designed to address the unique risks surrounding the contractor accounts; (ii) implement procedures to enforce these policies; and (iii) provide adequate technological, operational and administrative guidance to its employees and contractors on these very policies.

The lessons learned here are straightforward. First, Cybersecurity policies cannot be stagnant. Any responsible investment adviser would consider the prior attacks on the contractors' credentials as a material event that should warrant a revisit of its policies and controls. Furthermore, the constant change of technology, the evolving operational threat vectors and the growing sophistication of actual attacks on advisers, all command a periodic review of its Cybersecurity policies. Second, comprehensive and well-drafted policies must be integrated into actual procedures that are recorded and demonstrable and, most importantly, specifically curated and contoured to meet the specific attributes and corresponding unique Cyber risks faced by each firm. These policies will actually serve to a firm's detriment if they aspire to achieve certain controls that the firm cannot demonstrate are actually in place and are being periodically reviewed. Third, with the uptick in Cybersecurity resources at the Commission, such as the new Cyber Unit enforcement division and the third and fourth Cybersecurity sweeps currently underway at the time of this writing, no firm should think that actual investor harm is the condition precedent for building its Cybersecurity program – every registered investment adviser (including both exempt reporting advisers and nonregistered investment advisers) needs to have an appropriate Cybersecurity program in place as a cost of doing business. In the end, Voya agreed to settle the action by paying a fine of $1,000,000 and agreeing to certain remedial sanctions.

Takeaways for Practitioners – Practical Advice for Counseling PE Funds and PE Managers on Cybersecurity Compliance

In light of the foregoing, advisers to PE Funds and/or PE Managers must understand that Cybersecurity compliance requires an appreciation for both the long-standing statutory and regulatory framework as well as the Commission's more nuanced approach to data protection. Whereas the former can be distilled to a core standard of designing a Cybersecurity Program that is reasonably designed to protect data, the latter is an evolving standard that will continue to change over time, and rightfully so. What is clear today is that the regulatory crosshairs are firmly set on Cybersecurity compliance and every PE Manager must have controls in place that correspond to the Cyber Six, in order to survive a basic OCIE Cybersecurity examination (or an investor Operational Due Diligence examination for that matter). Moreover, as cyber-attacks and hacking initiatives grow in scope, sophistication, and frequency, so too will the expectations of what is considered a minimum standard of care in defending against and responding to cyber-attacks. For example, merely five years ago, a PE Fund or a PE Manager that had no Cybersecurity Program in place would cause little concern. However, today, the absence of such a program would undoubtedly constitute negligence per se in the eyes of both regulators overseeing PE Funds and PE Managers and the investors who fund them. For those attorneys charged with counseling PE Funds and PE Managers, a fundamental understanding of this newly formed and developing legal and regulatory landscape is essential.

Related Content

For additional information on regulatory and compliance matters applicable to private equity funds and their managers, see the following practice notes:

- Investment Advisers Act Key Provisions
- SEC Enforcement Priorities for Private Equity Firms
- Investment Adviser Custodial Practice Regulation
- Registered Investment Adviser: Reviewing a Compliance Program
- Investment Adviser Privacy Regulations
- Anti-Money Laundering Considerations for Private Equity Funds

About the Author

John Araneo is the Managing Director of Align Cybersecurity and also serves as the General Counsel of Align. John also remains a practicing attorney in the investment management space, has launched countless private investment vehicles and counsels his clients on the routine legal, operational and compliance matters facing private funds.

Having followed the regulatory initiative on Cybersecurity in the investment management space since its inception, John is an established author, Cybersecurity expert and well-known thought leader on the legal, regulatory and governance issues related to Cybersecurity.

Align *is a leading global provider of Technology Infrastructure Solutions, Managed IT Services, Professional Services and Data Center Solutions. For more than 30 years, our team has continuously invested in and expanded our strategic solutions to ensure our clients' technologies are cutting-edge and secure, and their IT environments are designed to enable seamless growth and meet evolving needs.*

Contact Us

Align
55 Broad Street
6th Floor
New York, NY 10004
212.207.2600
jaraneo@align.com