MorrisonCohen LLP

Client Alert

## SEC SETS BASELINE FOR INVESTMENT MANAGER CYBERSECURITY COMPLIANCE

February 6, 2020. Building on the results of thousands of field examinations conducted over the past few years, the SEC's Office of Compliance Investigations and Examinations formally put investment advisers on notice last week that it expects them to have in place a variety of policies, procedures and practices designed to protect the integrity of the data generated and used in their businesses.

OCIE made it clear that an adviser's failure to adhere to a well-considered mix of controls and procedures appropriate to the advisor's size, complexity and risk profile would be considered a failure to comply with the adviser's regulatory obligations. Additionally, OCIE was clear that simple reliance on outside services would not by itself be a sufficient exercise of an adviser's duties to its clients.

OCIE grouped the practices into seven broad functional (and to some extent overlapping) categories, emphasizing the dynamic an ongoing nature of the adviser's duty to review, update, revise and maintain them. Briefly, they are:

- Governance and Risk Management – ensuring that senior management was properly informed, engaged in and focused on the importance of inculcating across the organization a comprehensive culture of security; assessing and managing how the nature of the organization increased or reduced the risk that data could be compromised; and communicating to and training personnel, and then implementing and regularly testing, procedures designed to mitigate those risks.

- Access Rights and Controls – ensuring that the adviser understands the different types of data it acquires or generates, such as, for example, data pertaining to clients, investors, service providers, consultants, or investments and then implements

electronic, physical or other means to control how and by whom that data may be accessed or processed, including by such techniques as needs-based access-control privileges that are renewed or limited as circumstances warrant, greater focus on the hiring, training and termination process as it impacts data access, requiring multiple executive authorizations for access to more highly sensitive data, requiring user multi-factor authentication across platforms, and regularly monitoring data access to ensure compliance with policies, procedures and restrictions.

- Data Loss Prevention – ensuring that data are protected from unauthorized access, alteration, compromise, or removal. OCIE focused on such techniques as secure encryption of data both at rest and in transmission, electronically segmenting and isolating data by type or purpose, continuously monitoring the integrity of the network from outside or inside intrusion or threat, and ensuring that the organization continually updates all operating systems, application and security software and decommissions outdated systems.

- Mobile Security – recognizing that remote devices, such as laptops, tablets and smartphones, have the potential to serve as a vector for unauthorized access into an adviser's critical information systems, OCIE favorably noted organizations that apply their access control and data loss prevention principles to offsite data control, such as by restricting copying printing or downloading of data, and maintaining current inventory of and access controls over remote devices.

- Incident Response and Resiliency – ensuring that an adviser takes appropriate steps to harden its business against the risk of systemic failure and to recover quickly if it occurs, and have, and regularly test, clear written procedures to test vulnerability and recovery. Consistent with breach notification laws generally, OCIE highlighted the importance of those portions of the written plans designed to deal with data breach and exfiltration, including appropriately prompt communication of the breach to regulators and affected parties.

- Vendor Management – ensuring that the adviser conducts advance and ongoing diligence on all third parties who interface with the advisor, whether specifically for data management or processing purposes, or who merely have electronic connectivity of some sort to the manager's infrastructure, to ensure that their systems do not compromise the advisor's own. This might involve independent third party audit certification such as SOC 2, physical inspection, or written inquiry.

- Training and Awareness – by separately focusing on the adviser's duty to maintain a robust and ongoing program of user awareness training covering all of

aspects of data security relevant to the user's function, OCIE highlighted that the human factor remains the weakest link in any cybersecurity compliance regime.

To discuss any particular questions relating to the implication of OCIE's guidance or its implementation, please contact a member of Morrison Cohen's Technology, Data Privacy and Intellectual Property Group, or its Corporate Department.


Jessica Lipson
(212) 735-8683
jlipson@morrisoncohen.com

Henry Zangara
(212) 735-8859
hzangara@morrisoncohen.com

Shruti Chopra
(212) 735-8628
schopra@morrisoncohen.com

Jessica Colombo
(212) 735-8753
jcolombo@morrisoncohen.com