December 18, 2018

SEC Issues Risk Alert on Adviser Personnel's Use of Electronic Messaging

On December 14, 2018, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert to share its observations from a recent exam initiative that focused on investment adviser personnel's use of electronic messaging for business purposes. OCIE's examination initiative specifically highlighted whether and to what extent advisers complied with the relevant rules – including Rule 204-2 (the "Books and Records Rule") and Rule 204-2(a)(11) (the "Advertisements Recordkeeping Rule") – and whether advisers had adopted and implemented relevant policies and procedures to comply with their obligations under the Books and Records Rule and the Advertisements Recordkeeping Rule.

Most notably, in the Risk Alert, OCIE acknowledged the ability of adviser personnel to use personal devices, social media and texting/IM for business purposes, provided the adviser maintained policies and procedures to comply with the relevant regulations. OCIE also suggested some "best practices" with regards to the use of mobile and personally owned devices, including:

Policies and Procedures

- Prohibiting business use of apps and other technologies that (i) allow an employee to send messages or otherwise communicate anonymously, (ii) delete messages automatically, or (iii) prohibit third-party viewing or back-up.
- Adopting procedures that require an employee, who receives an electronic message for business purposes via a prohibited form of communication, to move the message to another electronic system that the adviser determines can be used in compliance with its record-keeping obligations.
- Adopting and implementing specific policies and procedures addressing the use of personally owned mobile devices for business purposes with respect to, for example, social media, instant messaging, texting, personal email, personal websites, and information security.
- Adopting and implementing policies and procedures for the monitoring, review, and retention of electronic communications for business purposes made via social media, personal email accounts, or personal websites.

Employee Training and Attestations

- Training all personnel on the adviser's policies and procedures regarding electronic messaging and providing regular reminders of those policies and procedures.
- Obtaining from all personnel attestations to their completion of the training and continued compliance with the adviser's policies and procedures.
- Assessing the adviser's risk on an ongoing basis by soliciting feedback from employees regarding the forms of electronic messaging requested by clients and service providers.

Supervisory Review

- For advisers that permit use of social media, personal email, or personal websites for business purposes, contracting with software vendors to (i) monitor the social media posts, emails, or websites, (ii) archive these

business communications to ensure compliance with record retention rules, and (iii) ensure that they have the capability to identify any changes to content and compare postings to a lexicon of key words and phrases.

- Regularly reviewing popular social media sites to identify if employees are using the media in a way not permitted by the adviser's policies.

- Running regular internet searches or setting up automated alerts to notify the adviser when an employee's name or the adviser's name appears on a website to identify potentially unauthorized advisory business being conducted online.

- Establishing a reporting program or other confidential means by which employees can report concerns about a colleague's electronic messaging, website, or use of social media for business communications.

Control Over Devices

- Loading certain security apps or other software on company-issued or personally owned devices prior to allowing them to be used for business communications. For instance, software is available that enables advisers to (i) "push" mandatory cybersecurity patches to the devices to better protect the devices from hacking or malware, (ii) monitor for prohibited apps, and (iii) "wipe" the device of all locally stored information if the device were lost or stolen.

- Allowing employees to access the adviser's email servers or other business applications only by virtual private networks or other security apps to segregate remote activity to help protect the adviser's servers from hackers or malware.

The Risk Alert suggests that it is a good time to review your firm's practices, as well as policies and procedures, concerning the use of personal devices, social media and texting/IM for business purposes. Ropes & Gray attorneys have considered these issues carefully. Please feel free to contact any member of Ropes & Gray's asset management practice groups or your usual Ropes & Gray contact with any questions about this Alert.