OCIE Pings Advisers on Electronic Messaging Best Practices

December 21, 2018

On December 14, 2018, the Office of Compliance Inspections and Examinations ("OCIE") of the U.S. Securities and Exchange Commission ("SEC") released a risk alert ("Risk Alert") describing recently observed best practices for registered investment advisers to consider when the adviser or its employees conduct business through electronic communications.[1] The Risk Alert is a timely reminder for advisers to evaluate their use of electronic messaging and update their policies and procedures to reflect current practices and ensure compliance. Investment advisers should (i) ensure that they are preserving all electronic communications (including communications that are not made through the corporate e-mail system, such as text messages from personal devices and messaging services and applications) as required by the Investment Advisers Act of 1940 (the "Advisers Act") and (ii) adopt and implement policies and procedures concerning permitted forms and uses of electronic communications, as tailored for the specific facts and circumstances of the investment adviser.

Debevoise & Plimpton

The Risk Alert followed a limited-scope or "sweep" examination initiative commenced in 2017 "designed to obtain an understanding of the various forms of electronic messaging used by advisers and their personnel, the risks of such use, and the challenges in complying with" the Advisers Act. In particular, the SEC staff focused on electronic communications that were not conducted through a firm's e-mail system, including text messaging, instant messaging, personal e-mail and personal or private messaging both on the adviser's corporate systems and devices and also third-party systems and personal devices.

DUTIES UNDER THE ADVISERS ACT

An investment adviser's compliance obligations under the Advisers Act regarding electronic communications are generally related to the recordkeeping rule (Rule 204-2) and the compliance rule (Rule 206(4)-7). Rule 204-2 includes the requirement to retain,

[1] U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Observations from Investment Adviser Examinations Relating to Electronic Messaging (Dec. 14, 2018), *available* here.

among other things, written communications relating to "any recommendation made or proposed to be made and any advice given or proposed to be given" and "the performance or rate of return of any or all managed accounts or securities recommendations."[2] Rule 206(4)-7 requires advisers to "[a]dopt and implement written policies and procedures reasonably designed to prevent violation [of the Advisers Act] by [the adviser] and [its] supervised persons."[3] Such policies and procedures should address "[t]he accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction."[4] The SEC has previously stated that, "regardless of whether information is delivered in paper or electronic form, broker-dealers and investment advisers must reasonably supervise firm personnel with a view to preventing violations."[5]

BEST PRACTICES

Based on its examinations, OCIE identified the following examples of best practices:

- *Limit Forms of Communication*. Restrict forms of electronic communications to only those that may be used in compliance with applicable rules and that are captured by the adviser's recordkeeping system. Firms thus might consider prohibiting the use of devices, applications or other technologies that can be more easily misused, such as those that permit anonymous communication or automatic destruction of communications or prohibit third-party viewing or back-up. If an employee receives business communications from such a platform, require the employee to move those communications to the firm's system by, for example, forwarding a text received in an app or non-firm account to a corporate email account.

- *Establish Policies and Procedures for Personal Devices*. Where employees are using their personal devices for business purposes, adopt and implement policies and procedures to address the use of "social media, instant messaging, texting, personal email, personal websites, and information security." To segregate personal and business activities, firms should consider controlling access to firm e-mail servers or other business applications from personal devices by requiring prior approval or by granting access through a virtual private network or other secure app. For company-issued and personal devices, install software to allow the firm to "push" mandatory

---

2 Advisers Act Rule 204-2(a).

3 Advisers Act Rule 206(4)-7.

4 U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Compliance Programs of Investment Companies and Investment Advisers, Investment Act Release No. 2204 (Dec. 17, 2003), *available* here.

5 U.S. Securities and Exchange Commission, Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Advisers Act Release No. 1562 (May 9, 1996), *available* here.

patches that protect devices from hacking or malware, to monitor use of restricted applications, and to "wipe" devices that are reported lost or stolen.

- *Establish Policies and Procedures for the Business Use of Personal EMail, Personal Websites and Social Media*. Where employees "use social media, personal email accounts or personal websites for business purposes," adopt and implement policies and procedures for "monitoring, review, and retention of such electronic communications."[6] These policies and procedures may include (i) employing third parties to monitor use of social media, personal email or personal websites and to archive business communications; (ii) performing regular reviews of social media sites to ensure compliance with policies, and (iii) creating automated alerts to notify compliance staff "when an employee's name or the adviser's name appears on a website."

The adviser's compliance policies should cover the following elements:

- *Monitoring*. Establish and implement policies and procedures to monitor the use of electronic communications, including on personal devices and in personal e-mail and social media accounts.

- *Training*. Establish and require training on policies and procedures that inform employees of the limits of allowable electronic messaging use and the disciplinary consequences for misuse.

- *Confidential Reporting*. Create systems to allow for confidential reporting of violations.

- *Attestations of Compliance*. Ensure completion of training and compliance with policies and procedures by obtaining employee attestations at the commencement of their employment and at regular intervals.

- *Tailor and Update Policies for Specific Risks*. Understand what forms of electronic communications are used by employees and requested by clients in order to assess individual risks and update policies and procedures accordingly.

- *Inform Employees of Consequences*. Inform employees that "violations may result in discipline or dismissal" and adopt and implement policies and procedures that include such a statement.

---

[6] *See also*, U.S. Securities and Exchange Commission, Investment Advisers Use of Social Media (Jan. 4, 2012), *available* here.

The Risk Alert is a timely reminder to firms to review their policies with respect to electronic communications, including employee use of text messaging and other messaging applications. Please do not hesitate to contact us with any questions.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Kenneth J. Berman
kjberman@debevoise.com

WASHINGTON, D.C.

Kara Brockmeyer
kbrockmeyer@debevoise.com

WASHINGTON, D.C.

Robert B. Kaplan
rbkaplan@debevoise.com

WASHINGTON, D.C.

Julie M. Riewe
jriewe@debevoise.com

WASHINGTON, D.C.

Gregory T. Larkin
gtlarkin@debevoise.com

NEW YORK

Norma Angelica Freeland
nafreeland@debevoise.com