NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations[*]

Observations from Investment Adviser Examinations Relating to Electronic Messaging

I. Introduction

Key takeaway. *OCIE encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with applicable regulatory requirements.*

The Office of Compliance Inspections and Examinations ("OCIE") conducted a limited-scope examination initiative of registered investment advisers ("advisers") 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 certain provisions of the Investment Advisers Act of 1940 ("Advisers Act"). OCIE conducted this initiative because it noticed an increasing use of various types of electronic messaging by adviser personnel for business-related communications.[1]

The purpose of this Risk Alert is to remind advisers of their obligations when their personnel use electronic messaging and to help advisers improve their systems, policies, and procedures by sharing the staff's observations from these examinations.

II. Relevant Regulation

Advisers Act Rule 204-2 ("Books and Records Rule") requires advisers to make and keep certain books and records relating to their investment advisory business, including typical accounting and other business records as required by the Commission. For example, Rule 204-2(a)(7) requires advisers to make and keep "[o]riginals of all written communications received and copies of all written communications sent by such investment adviser relating to (i) any recommendation made or proposed to be made and any advice given or proposed to be given, (ii) any receipt, disbursement or delivery of funds or securities, (iii) the placing or execution of any order to purchase or sell any security, or (iv) the performance or rate of return of any or all managed accounts or securities recommendations," subject to certain limited exceptions.

Additionally, Rule 204-2(a)(11) requires advisers to make and keep a copy of each notice,

---

[*] The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the "SEC" or the "Commission") has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

[1] Numerous articles also have been written on electronic messaging trends and the compliance challenges that they may pose. *See e.g.*, Jackie Noblett, *SMH: Texting, Chat Continue to Vex Compliance Depts.*, IGNITES (June 2, 2017) and Jason Wallace, *Text Messaging: The Communication Risk Compliance Fears Most – Survey*, REGULATORY INTELLIGENCE (May 26, 2017).

circular, advertisement, newspaper article, investment letter, bulletin or other communication that the investment adviser circulates or distributes, directly or indirectly, to ten or more persons. The Commission has 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."[2]

Advisers Act Rule 206(4)-7 ("Compliance Rule") requires advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and rules thereunder.[3] According to the Compliance Rule's adopting release, each adviser should identify compliance factors creating risk exposures for the firm and its clients in light of the adviser's particular operations, and then design policies and procedures that address those risks.[4] The Commission stated that an adviser's policies and procedures should address, to the extent relevant to the adviser, "[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," among other things.[5] The Compliance Rule also requires an adviser to review, no less frequently than annually, the adequacy of the adviser's compliance policies and procedures and the effectiveness of their implementation.

As discussed below, a number of changes in the way mobile and personally owned devices are used pose challenges for advisers in meeting their obligations under the Books and Records Rule and the Compliance Rule.[6] These changes include the increasing use of social media, texting, and other types of electronic messaging apps, and the pervasive use of mobile and personally owned devices for business purposes.

III. Scope of Electronic Messaging Covered by the Examinations

OCIE's examinations surveyed firms to learn the types of electronic messaging used by firms and their personnel,[7] and reviewed firms' policies and procedures to understand how advisers were addressing the risks presented by evolving forms of electronic communication. For purposes of this initiative, "electronic messaging" or "electronic communication" included

---

[2] *Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information*, Advisers Act Rel. No. 1562 (May 9, 1996), *available at* https://www.sec.gov/rules/interp/33-7288.txt.

[3] Advisers Act Rule 206(4)-7(a).

[4] *Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Release No. 2204 (Dec. 17, 2003) at Section II.A.1., *available at* http://www.sec.gov/rules/final/ia-2204.htm.

[5] *See id.* at n.19 and accompanying text.

[6] This Risk Alert is not intended to be a comprehensive overview of all applicable regulatory requirements. The use of electronic messaging may implicate regulations beyond those specifically discussed in this Risk Alert.

[7] Adviser legal and regulatory requirements generally cover persons associated with an adviser, which can include many types of advisory personnel – such as employees, independent contractors, and investment adviser representatives. For purposes of this Risk Alert, the terms "personnel," "employees," and "representatives" are used interchangeably and include independent contractors.

written business communications conveyed electronically using, for example, text/SMS messaging, instant messaging, personal email, and personal or private messaging. OCIE included communications when conducted on the adviser's systems or third-party applications ("apps") or platforms or sent using the adviser's computers, mobile devices issued by advisory firms, or personally owned computers or mobile devices used by the adviser's personnel for the adviser's business.

The staff specifically excluded email use on advisers' systems from this review because firms have had decades of experience complying with regulatory requirements with respect to firm email, and it often does not pose similar challenges as other electronic communication methods because it occurs on firm systems and not on third-party apps or platforms.

IV. Summary of Examination Observations

OCIE's examination initiative focused on whether and to what extent advisers complied with the Books and Records Rule and adopted and implemented policies and procedures as required by the Compliance Rule. During the course of the initiative, the staff observed a range of practices with respect to electronic communications, including advisers that did not conduct any testing or monitoring to ensure compliance with firm policies and procedures. The staff observed and identified the following examples of practices[8] that the staff believes may assist advisers in meeting their record retention obligations under the Books and Records Rule and their implementation and design of policies and procedures under the Compliance Rule:

Policies and Procedures

- Permitting only those forms of electronic communication for business purposes that the adviser determines can be used in compliance with the books and records requirements of the Advisers Act.
- Specifically prohibiting business use of apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up.
- In the event that an employee receives an electronic message using a form of communication prohibited by the firm for business purposes, requiring in firm procedures that the employee move those messages to another electronic system that the adviser determines can be used in compliance with its books and records obligations, and including specific instructions to employees on how to do so.
- Where advisers permit the use of personally owned mobile devices for business purposes, adopting and implementing policies and procedures addressing such use

[8] This Risk Alert is not intended to be a comprehensive list of practices for a firm to meet its regulatory obligations, but rather to provide a sample of practices staff observed that may be helpful to advisers assessing their compliance policies and procedures addressing electronic messaging, including with respect to recordkeeping, supervision, or cybersecurity.

with respect to, for example, social media, instant messaging, texting, personal email, personal websites, and information security.

- If advisers permit their personnel to use social media, personal email accounts, or personal websites for business purposes, adopting and implementing policies and procedures for the monitoring, review, and retention of such electronic communications.

- Including a statement in policies and procedures informing employees that violations may result in discipline or dismissal.

Employee Training and Attestations

- Requiring personnel to complete training on the adviser's policies and procedures regarding prohibitions and limitations placed on the use of electronic messaging and electronic apps and the adviser's disciplinary consequences of violating these procedures.

- Obtaining attestations from personnel at the commencement of employment with the adviser and regularly thereafter that employees (i) have completed all of the required training on electronic messaging, (ii) have complied with all such requirements, and (iii) commit to do so in the future.

- Providing regular reminders to employees of what is permitted and prohibited under the adviser's policies and procedures with respect to electronic messaging.

- Soliciting feedback from personnel as to what forms of messaging are requested by clients and service providers in order for the adviser to assess their risks and how those forms of communication may be incorporated into the adviser's policies.

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 such 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. Such policies included prohibitions on using personal social media for business purposes or using it outside of the vendor services the adviser uses for monitoring and record retention.

- 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. Particularly with respect to social media, colleagues may be "connected" or "friends" with each other and see questionable or impermissible posts before compliance staff notes them during any monitoring.

Control over Devices

- Requiring employees to obtain prior approval from the adviser's information technology or compliance staff before they are able to access firm email servers or other business applications from personally owned devices. This may help advisers understand each employee's use of mobile devices to engage in advisory activities.

- Loading certain security apps or other software on company-issued or personally owned devices prior to allowing them to be used for business communications. 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.

V. Conclusion

In sharing its observations from this examination initiative, OCIE encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with their regulatory requirements. OCIE also encourages advisers to stay abreast of evolving technology and how they are meeting their regulatory requirements while utilizing new technology.

While this initiative was limited to examinations of investment advisers and this Risk Alert only references regulatory provisions under the Advisers Act, other types of regulated financial services entities may face similar challenges with new communication tools and methods.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.