To Our Clients and Friends

Memorandum

OCIE Publishes Risk Alert Regarding Electronic Messaging

On December 14, 2018, the Office of Compliance Inspections and Examinations ("OCIE") published its fifth National Exam Program Risk Alert (the "Risk Alert") this year to remind advisers of their obligations with respect to the use of electronic messaging by their personnel and to help advisers improve their systems, policies, and procedures around electronic messaging.[1] OCIE published the Risk Alert following a limited-scope examination initiative of registered investment advisers (the "Initiative"). The Initiative was designed to help OCIE gain an understanding of the various forms of electronic messaging used by advisers and their personnel, the risks of such uses, and the challenges posed by such electronic messaging in complying with certain provisions of the Investment Advisers Act of 1940 (the "Advisers Act"). Rather than highlighting frequent deficiencies, the Risk Alert summarizes examples of practices that OCIE believes may assist advisers in meeting their obligations under the Advisers Act.

In connection with the Initiative, OCIE examined communications that were conducted on the adviser's systems or third-party applications ("apps") or platforms, as well as communications sent using the adviser's computers, firm-issued mobile devices, and personal computers and mobile devices used by personnel for the adviser's business.[2] The Initiative focused on whether and to what extent advisers complied with Advisers Act Rule 204-2 (the "Books and Records Rule") and adopted and implemented policies and procedures as required by Advisers Act Rule 206(4)-7 (the "Compliance Rule") with respect to such communications.

The Books and Records Rule requires advisers to make and keep certain books and records relating to their investment advisory business, including, for example, "[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. The Securities and Exchange Commission ("SEC") has stated that, "regardless of whether information is delivered in paper or electronic

---

1 National Exam Program Risk Alert, Observations from Investment Adviser Examinations Relating to Electronic Messaging (Dec. 14, 2018), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf.

2 OCIE stated in the Risk Alert that it specifically excluded email use from the Initiative because firms have had decades of experience complying with regulatory requirements with respect to firm email, and because email often does not pose similar challenges as other electronic communication systems.

Copyright © 2018 Fried, Frank, Harris, Shriver & Jacobson LLP
A Delaware Limited Liability Partnership

form, broker-dealers and investment advisers must reasonably supervise firm personnel with a view to preventing violations."[3]

The Compliance Rule requires advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and Advisers Act rules. 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 SEC 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.

OCIE noted that the increased 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 pose challenges for investment advisers in meeting their obligations under both the Books and Records Rule and the Compliance Rule. The practices that OCIE identified as potentially helpful to advisers are summarized below.

1. *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 (e.g., apps and other technologies that allow anonymous communication or automatic destruction of messages, or that prohibit third-party viewing or back-up).
   - Requiring that electronic messages received using a prohibited form of communication be moved to another electronic system that the adviser determines can be used in compliance with its books and records obligations, and including specific instructions on how to do so.
   - Adopting and implementing 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.

---

[3] 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 at* https://www.sec.gov/rules/interp/33-7288.txt.

[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] *Id*.

- Adopting and implementing policies and procedures for the monitoring, review, and retention of electronic communications by adviser personnel on social media, personal email accounts, or personal websites for business purposes.

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

2. *Employee Training and Attestation*

   - Requiring personnel to complete training on the adviser's policies and procedures regarding the use of electronic messaging and electronic apps.

   - 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.

3. *Supervisory Review*

   - Contracting with software vendors to (i) monitor social media posts, personal emails, or personal websites used by personnel for business purposes, (ii) archive such business communications to ensure compliance with record retention rules, and (iii) ensure that any changes to content can be identified and postings can be compared 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 for the appearance of an employee's name or the adviser's name 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.

4. *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.

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

- Allowing employees to access the adviser's email servers or other business applications only by virtual private networks or other security apps.

The Risk Alert encourages investment advisers to review their risks, practices, policies, and procedures regarding electronic messaging, to consider any improvements to their compliance programs, and to stay abreast of evolving technology and how they are meeting their regulatory requirements while utilizing new technology. While the Risk Alert indicates that OCIE acknowledges the difficulties advisers face in complying with the Books and Records Rule and the Compliance Rule with respect to electronic messaging, as with other OCIE risk alerts, this Risk Alert could serve to signal the industry that the SEC is unlikely to be lenient in future enforcement cases regarding compliance with these rules with respect to electronic messaging. Therefore, all investment advisers should review their current practices and compare their policies and procedures against the practices identified in the Risk Alert.

* * *

Authors:

Jessica Forbes

Stacey Song

Joanna D. Rosenberg

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its contents. If you have any questions about the contents of this memorandum, please call your regular Fried Frank contact or an attorney listed below:

Contacts:

London		
Gregg Beechey	+44.20.7972.9172	gregg.beechey@friedfrank.com
David Christmas	+44.20.7972.9222	david.christmas@friedfrank.com
Kate Downey	+44.20.7972.6221	kate.downey@friedfrank.com
Mark Mifsud	+44.20.7972.9155	mark.mifsud@friedfrank.com
David W. Selden	+44.20.7972.6201	david.selden@friedfrank.com
Sam Wilson	+44.20.7972.9223	sam.wilson@friedfrank.com
New York		
Jonathan S. Adler	+1.212.859.8662	jonathan.adler@friedfrank.com
Lawrence N. Barshay	+1.212.859.8551	lawrence.barshay@friedfrank.com
Jeremy R. Berry	+1.212.859.8796	jeremy.berry@friedfrank.com
Gerald H. Brown, Jr.	+1.212.859.8825	gerald.brown@friedfrank.com
Jessica Forbes	+1.212.859.8558	jessica.forbes@friedfrank.com
Darren A. Littlejohn	+1.212.859.8933	darren.littlejohn@friedfrank.com
Robert M. McLaughlin	+1.212.859.8963	robert.mclaughlin@friedfrank.com
Todd J. McMullan	+1.212.859.8190	todd.mcmullan@friedfrank.com
David S. Mitchell	+1.212.859.8292	david.mitchell@friedfrank.com
Kenneth I. Rosh	+1.212.859.8535	kenneth.rosh@friedfrank.com
Lisa M. Schneider	+1.212.859.8784	lisa.schneider@friedfrank.com
Stacey Song	+1.212.859.8898	stacey.song@friedfrank.com
Washington, D.C.		
Richard I. Ansbacher	+1.202.639.7065	richard.ansbacher@friedfrank.com
William J. Breslin	+1.202.639.7051	william.breslin@friedfrank.com
Walid Khuri	+1.202.639.7013	walid.khuri@friedfrank.com
Bradford R. Lucas	+1.202.639.7483	brad.lucas@friedfrank.com
Andrew P. Varney	+1.202.639.7032	andrew.varney@friedfrank.com
Rebecca N. Zelenka	+1.202.639.7260	rebecca.zelenka@friedfrank.com