CONSTELLATION ADVISERS, LLC

REGULATORY NOTICE: 19-01

DON'T FAIL TO REVIEW AND RETAIN THE SEC'S WARNINGS IN ITS RECENT RISK ALERT REGARDING ELECTRONIC MESSAGING

The Office of Compliance Inspections and Examinations ("OCIE") recently issued a Risk Alert highlighting investment advisers' obligations when their personnel use electronic messaging. The full text of the Risk Alert is available here. Among other things, Rule 204-2 of the Advisers Act ("Books and Records Rule") currently requires advisers to maintain certain books and records, which includes electronic records such as emails and other electronic messaging used for business-related communications. In addition, Rule 204-2(a)(7) requires advisers, subject to certain limited exceptions, to make and keep originals of all written communications received and copies of all written communications sent by investment advisers relating to the following:

- Any recommendation made or proposed to be made and any advice given or proposed to be given;
- Any receipt, disbursement or delivery of funds or securities;
- Placing or execution of any order to purchase or sell any security; and
- Performance or rate of return of any or all managed accounts or securities recommendations.

Whether the communications related to an investment adviser's business are electronic or in a paper format, the adviser must reasonably supervise firm personnel to prevent violations of regulatory obligations. Several recent 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 Rule 206(4)-7 ("Compliance Rule").

The Staff's suggestions to advisers to best comply with existing law include:

Policies and Procedures

- Establish policies and procedures prohibiting the business use of third-party applications ("apps") that prevent the employee from being identified or the messages from being tracked, saved, or viewed by third parties;
- Establish policies and procedures with respect to business activities over social media, texting, personal email, and personal websites;
- Establish a protocol for employees to follow in a situation where they are contacted about business matters through a prohibited messaging platform; and
- Inform employees through the adviser's policies and procedures that violations of these guidelines around electronic messaging may result in disciplinary action or dismissal.

Employee Training and Attestations

- Require employees to complete training on the adviser's policies and procedures on electronic messaging, and obtain attestations from them;

- Periodically remind employees of company policies and procedures around electronic messaging; and
- Survey personnel to determine popular messaging forms requested by clients and service providers, and then develop specific policies around those platforms.

Supervisory Review

- Monitor and archive communications made over social media, personal email, or personal websites;
- Regularly review popular social media sites, run Internet searches, and set up automated alerts on employees' names to identify possible violations of the adviser's electronic messaging policies and to identify potentially unauthorized advisory business being conducted online; and
- Establish confidential means by which employees can report a colleague's improper use of electronic messaging.

Control Over Devices

- Create measures that require employees to obtain approval before accessing firm servers on personally-owned devices;
- Load security apps on both company-issued and personally-owned devices to better prevent hacking, monitor prohibited apps, or erase locally stored information in the event the device is lost or stolen; and
- Grant access to company servers only by virtual private networks to protect against hackers

TAKE ACTION!

Clients Should:

- Inventory the methods of electronic communications your firm's personnel use to communicate with clients and investors, including text/SMS messaging, instant messaging, personal email, and personal or private messaging services or applications.
- Determine what platforms firm personnel will be permitted to use to communicate with clients and investors (e.g. apps, mobile devices or computers issued by advisory firms, or personally owned computers or mobile devices).
- Confirm all methods and platforms used to communicate firm business are being retained and monitored.
- Develop policies and procedures and testing protocols to:
    - Prohibit and/or detect use of methods and platforms for which the firm is not retaining communications;
    - Supervise firm personnel's use of approved platforms and communication methods;
    - Monitor for firm personnel's use of unapproved communication platforms and methods; and
    - Review the policies and procedures during the firm's annual review.

Contact a member of Constellation's compliance team for assistance with developing or implementing any of these suggested actions.