OCIE Scrutinizing Electronic Communications

An Overview of the Latest Requests and Tips to Be Examination-Ready.

Written by
Molly Rowan, Assistant Vice President, Cordium

The SEC this week has signaled that OCIE's attention has turned to advisers' use of electronic messaging. Several clients received sweep exam requests specifically targeting electronic communications on advisers' systems or on third-party applications. These requests are explicitly *not* focused on firm-provided email accounts, but rather on other electronic messages (e.g. text messages, social media messages, third-party apps such as Slack or Bloomberg, personal emails, etc.).

The following provides an overview of the requested documentation:

Background Information

In response to the recent examinations, registrants should be prepared to describe employee use of electronic messaging services or platforms, as well as the specific devices and applications used.

The very first step in crafting a compliance program is assessment. Before you can adequately develop policies, procedures, and a supervisory process, you need to fully understand how your employees are utilizing electronic communications to conduct firm business. One approach is to utilize compliance questionnaires and notifications to ascertain what accounts employees have and whether or not they are using them for business purposes. Once employee use is determined, ensure required records are adequately retained. The firm's electronic communications policies and procedures should contemplate each and every platform and type of communication utilized by employees.

Compliance Program

The SEC is requesting copies of written or informal policies and procedures concerning the use of electronic communications, as well as a description and evidence of any ongoing monitoring of firm electronic messaging. The requests also look for documentation related to any detected violations or exceptions and actions taken. OCIE is focused on any risk assessments conducted by the adviser related to electronic messaging and the mitigation of any identified risks.

These requests tell us two things: (i) the SEC is looking for policies and procedures that broadly address electronic communications, not just firm e-mail, and (ii) the review of communications should be part of your firm's supervisory process. In Cordium's view, this shifts electronic communication review from a "best practice" to a regulatory expectation, which may be the biggest take-away from this sweep request. If you are not already doing electronic communication reviews, you should build it into your compliance testing schedule.

It is worth noting that logging in and reviewing communications may not be enough. You should be testing the systems used for retention and documenting that they are functional in addition to documenting the reviews conducted along with any follow-ups with employees.

The fact that the SEC is looking for risk assessments concerning electronic communications and the mitigation of risks tells us that your reviews should be tailored based on that assessment. Our electronic communications review team accomplishes this by tailoring each client review based on the firm-specific strategy and risks. Your firm's risks should drive the search parameters behind your reviews.

Recordkeeping

OCIE is focused on the retention and maintenance of records related to electronic communications. This includes documentation around the devices, applications, and third-party vendors being used as well specifics around the retention of required records.

To the extent employees are utilizing *any* electronic messages to conduct firm business, your firm should have a mechanism for retaining and archiving those communications. The retention of the communications should be part of your firm's recordkeeping system, and there should be processes around ensuring the effectiveness of the controls around the retention. Most of your communications are housed by third-party vendors. Ensure you have records of any diligence conducted on those third-parties (e.g. did you ensure that the service provider has WORM functionality, which is required to be SEC-compliant?). Your policies should prohibit employee use of any communications for business purposes which are not already subject to your firm's supervision processes.

Security and Privacy of Information

Among the requested items are written policies and procedures related to the transmittal of sensitive information (e.g. non-public personal information) using electronic messaging.

Your firm's Written Information Security Policy should address the controls around use of electronic messaging. To the extent your employees are utilizing electronic messaging to communicate regarding firm business, it is likely such communications contain proprietary firm information or non-public personal information. The transmission of NPPI, specifically, is protected by various state and federal regulations, so it is imperative your information security policies address each and every platform utilized.

If you haven't done so already, Cordium can assist you in the development of policies and procedures around electronic messaging. Cordium's dedicated electronic communications review team has the expertise to build out a risk-specific supervision process, conduct your firm's electronic reviews, and *provide documentation to evidence your firm's commitment to the monitoring of electronic messaging. Please reach out to your Cordium contacts with any questions.*