IAA Today
powered by SmartBrief

Compliance Corner
May 9, 2024

Off-Channel Communications: Confronting Compliance Challenges

Lancelot A. King

Joseph Nardello

*Lancelot A. King and Joseph Nardello, Seward & Kissel LLP**

Employees of investment advisers have long used email as their primary means of business communication, but they are increasingly using other means, such as messaging applications and social media platforms, for business purposes. This evolution began with the rise of smartphones and seemingly accelerated due to the pandemic-related proliferation of remote work arrangements. In response, the SEC and its staff are showing a heightened focus on the use of electronic communications, particularly so-called "off-channel communications," by advisers and their employees.

This article outlines the compliance challenges associated with off-channel communications and discusses key considerations for advisers seeking to comply with their recordkeeping, supervisory, and other compliance obligations relating to off-channel communications.

What are off-channel communications?

The term "off-channel communications" refers to communications that are sent on applications, platforms, or devices that have not been approved by the adviser for business use. Off-channel

communications may include, for example, communications on messaging and chat applications (e.g., Bloomberg, Slack, Signal, WhatsApp, WeChat, Zoom), social media platforms (e.g., LinkedIn), text messages, and personal email.

What regulations apply to advisers with respect to off-channel communications?

The Investment Advisers Act of 1940 (Advisers Act) and the rules thereunder contain various provisions that apply to advisers with respect to off-channel communications, the most significant of which are:

- **Recordkeeping**: Rule 204-2 (Books and Records Rule) requires advisers to make and keep certain records. In particular, Rule 204-2(a)(7) requires an adviser to maintain all written communications received and copies of all written communications sent by the adviser relating to (among other things): any recommendations made or proposed to be made and any advice given or proposed to be given; any receipt, disbursement, or delivery of funds or securities; and the placing or execution of any order to purchase or sell any security. These requirements are noteworthy in that they focus on the content – rather than the form – of the communication.
- **Supervision**: Section 203(e)(6) authorizes the SEC to sanction advisers for failing to reasonably supervise personnel with a view to preventing violations of securities laws and provides that an adviser will not be deemed to have failed to reasonably supervise if it has (i) "established procedures, and a system for applying such procedures, which would reasonably be expected to prevent and detect, insofar as practicable, any such violation" and (ii) "reasonably discharged the duties and obligations incumbent upon [it] by reason of such procedures and system without reasonable cause to believe that such procedures and system were not being complied with" (emphasis added).
- **Policies and Procedures**: 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 the rules thereunder.

How has the SEC staff approached off-channel communications?

In December 2018, the SEC's examinations staff issued a Risk Alert regarding advisers' regulatory obligations relating to the use of electronic communications by their personnel. The Risk Alert notes that changes in the use of mobile and personal devices pose challenges for advisers with respect to the Books and Records Rule and the Compliance Rule. The Risk Alert also provides examples of practices that the staff believed could assist advisers in satisfying their recordkeeping obligations and in designing and implementing policies and procedures under the Compliance Rule. The examples focus on (i) policies and procedures, (ii) employee training and attestations, (iii) supervisory review, and (iv) adviser control over devices. (Best practices in these areas are discussed in "Compliance Considerations" below.)

In addition, the SEC's examinations staff has made electronic communications an exam priority. The staff stated in its "2023 Examination Priorities" report that it would review advisers' policies and

procedures for retaining and monitoring electronic communications. Indeed, during exams, the staff has been requesting information regarding electronic communications, including (i) whether advisers permit employees to use personal devices and forms of electronic communication other than adviser email accounts for business purposes, (ii) steps advisers take in approving the use of personal devices or non-email forms of electronic communications, and (iii) steps advisers take to ensure that employees only use approved forms of electronic communication for business purposes.

Has the SEC charged advisers with violations relating to off-channel communications?

Yes. Since 2021, the SEC has charged nearly 60 firms – including broker-dealers and their affiliated advisers, as well as dually registered firms – with violations relating to off-channel communications. Notably, in April 2024, the SEC announced its first off-channel communications enforcement action against a standalone adviser. The enforcement actions involving Advisers Act violations have included failures to preserve written communications as required by Rule 204-2(a)(7), failures to reasonably supervise personnel within the meaning of Section 203(e)(6), and – in the case of the standalone adviser – failure to *implement* policies and procedures as required by the Compliance Rule.

The settlement orders for these enforcement actions indicate that the advisers had adopted policies prohibiting off-channel communications, but employees violated the policies and the advisers failed to monitor and, as a result, failed to preserve employees' communications.

Settling the charges has been costly, as firms have agreed to pay multimillion-dollar penalties and retain independent compliance consultants to conduct comprehensive reviews of their policies and procedures, surveillance programs, training, and other matters.

Compliance Considerations

Many advisers adopt electronic communications policies requiring employees to use *only* approved platforms and devices for business communications, thereby prohibiting off-channel communications. However, the enforcement actions demonstrate that simply having such a policy, providing training, and obtaining attestations are not sufficient to satisfy an adviser's regulatory obligations. The SEC has focused on advisers' failures to reasonably supervise employees and resulting failures to preserve records, along with failures to *implement* policies and procedures. Accordingly, as discussed below, crafting an electronic communications policy warrants careful consideration — but that is only the starting point.

Policies and Procedures.

- ***Tailoring*.** The SEC has stated that an adviser should identify compliance factors creating risk exposure for the adviser and its clients in light of the adviser's particular operations, and then design policies and procedures that address those risks. In other words, policies should be tailored to the adviser's operations. Therefore, a reasonably designed policy should reflect the

adviser's understanding of its employees' communications practices. To develop an understanding of those practices, advisers can survey their employees (and perhaps even clients) to determine which communications channels they use or would prefer to use. Conducting surveys can assist the adviser in tailoring its policy – bolstering its view that the policy is reasonably designed – and can also assist in demonstrating the adviser's supervisory efforts.

- ***Scope of covered communications*.** Electronic communications policies are typically broadly written to cover "all business communications" or "all communications for business purposes," and usually do not define with much specificity the types of communications that are covered by the policy. This is mainly because the scope of the Books and Records Rule focuses on the content of the communication and, in places, is not entirely clear, particularly with respect to which communications are "relating to" recommendations or advice (within the meaning of Rule 204-2(a)(7)). Furthermore, the enforcement actions appear to have created some uncertainty as to how the SEC interprets the scope of the Books and Records Rule — in this regard, a common question is whether the Rule requires advisers to preserve communications that are purely internal (i.e., when both the sender and the recipient are adviser personnel and no external persons are involved). Therefore, when designing a policy that will govern innumerable communications sent each day, most advisers find it administratively easier – and less risky – to adopt a policy that broadly applies to all business communications. Such broad application relieves employees from having to use their own judgment about which communications are covered.
- ***Personal devices.*** Advisers are increasingly permitting employees to use personal devices for business purposes. An adviser that permits employees to use personal devices should consider how to monitor and preserve business communications. Advisers commonly require employees to install on their personal devices specialized software for hosting, capturing and archiving business communications. When selecting such software, advisers should be mindful of employees' privacy rights and applicable privacy laws. While advisers typically inform employees (in the policy and in training sessions) that they should have no expectation of privacy when using adviser-owned devices, advisers should likewise clarify what employees should expect regarding privacy when using their personal devices.

  An adviser that permits employees to use personal devices should also consider whether it will be able to implement all of its procedures relating to personal devices. For example, the settlement order for the enforcement action against the standalone adviser notes that although the adviser's policy permitted it to access personal devices to review for off-channel communications, the adviser did not access personal devices and did not monitor off-channel communications. The SEC found that the adviser failed to implement its procedures as required by the Compliance Rule.
- ***Occasional or inadvertent off-channel communications***. Advisers should consider how to treat instances where an employee receives a business communication off-channel. A common example is where a client normally communicates with the adviser via email but occasionally or

inadvertently sends off-channel text messages to an employee. Many advisers require employees to (i) forward such communications to an approved channel in a secure manner and (ii) notify the compliance department. In addition, an employee who receives an off-channel communication may wish to inform the sender of the adviser's policy and ask the sender to use an approved channel in the future.

- ***Ephemeral and encrypted messages.*** Advisers should prohibit the use of ephemeral (or "disappearing" or "auto-deleted") messages and encrypted messages that cannot be captured and archived. Signal, Slack, WeChat, and WhatsApp are examples of platforms that use encryption and/or have auto-delete functions that in some cases can be enabled. Ephemeral and encrypted messages may have security and privacy advantages but are not suitable for business communications to the extent they cannot be preserved.

Documentation. Advisers should document the steps they take in addressing risks relating to off-channel communications, and they should do so with an eye toward being able to demonstrate to the SEC staff (in an exam) that they took such steps. For example, advisers should maintain documentation regarding (i) their process and rationale for approving particular channels and devices, (ii) the steps taken in monitoring employees' communications, (iii) the results of compliance testing, (iv) training and attestations, (v) internal investigations, and (vi) disciplinary actions.

Monitoring. The SEC enforcement actions underscore the importance of monitoring whether employees are complying with electronic communications policies. Monitoring in the context of off-channel communications poses unique challenges, as advisers typically cannot access unapproved channels (e.g., WhatsApp messages on personal devices) and therefore have little or no visibility into whether employees are using those channels for business purposes. One common approach to monitoring is to review approved channels for evidence of off-channel communications by conducting keyword searches; for example, many advisers search their email systems for words and phrases that refer to or suggest off-channel communications (e.g., references to "text," "text message," or names of unapproved channels), and then use any findings to investigate whether off-channel communications have occurred. Such reviews should be conducted on a regular basis (ideally monthly or quarterly) and can be conducted efficiently using software programs, some of which can perform automated reviews. Finally, many advisers interview employees, inquiring about off-channel communications and changes in how employees are communicating — at the very least, such interviews may have a deterrent effect by impressing upon employees that the adviser actively seeks to enforce its policy.

Capturing and archiving. When considering which channels to approve, a key factor is whether the adviser will be able to capture and archive communications on the channel. Fortunately, there are a variety of technology solutions available. Many advisers employ third-party vendors or software to capture and archive communications on non-email channels. Some vendors have even developed technologies that can capture and archive certain types of ephemeral or encrypted messages.

Training. Advisers should provide employees with training on an ongoing basis, not just at the commencement of employment. The training should be designed to ensure that employees understand the adviser's electronic communications policy, with a particular emphasis on which channels are

approved and which are prohibited. The training should also educate employees on applicable regulations and the risks to the adviser's business – e.g., security risks, regulatory risks such as SEC sanctions, and reputational risks. Employees should be warned of potential disciplinary consequences. In addition, the training should remind employees to report any known or suspected policy violations and should encourage employees to contact the compliance department if any aspect of the policy is unclear. Finally, the training should reflect that proper use of electronic communications is a priority for the adviser.

Attestations. Advisers commonly require employees to sign attestations confirming that they understand and comply with policies. This is typically done at the commencement of employment and at least annually thereafter. To emphasize the gravity of risks relating to off-channel communications and to sharpen employees' focus on this area, an adviser may wish to use attestations that are specific to electronic communications, as opposed to using one attestation that covers the entire compliance manual. In addition, quarterly attestations can be more impactful than annual certifications. While some advisers use attestations that require only a signature and date, advisers should consider using a check-the-box format with questions about the employee's experiences — this approach can support the adviser's supervisory efforts by increasing opportunities for the compliance department to gain insight into employees' communications practices.

Discipline. Advisers should take appropriate disciplinary action when employees violate policies relating to electronic communications. Potential disciplinary consequences should be severe enough (e.g., termination of employment) to deter violations. Disciplinary action should be taken in a uniform manner, with senior management being held to the same standard as other employees.

Conclusion

The SEC has made clear its interest in having access to advisers' records in order to enforce federal securities laws, and the ongoing enforcement actions are furthering that interest. The recent enforcement action against the standalone adviser may be a precursor to more enforcement actions against advisers in the off-channel context, and it highlights the importance of *reasonably supervising* personnel and *implementing* policies and procedures. Approaching off-channel communications from a compliance perspective may seem like a daunting challenge, as advisers generally do not have access to unapproved channels. However, an adviser can seek to comply with applicable regulations by establishing a robust supervisory program comprised of multiple procedures (e.g., monitoring, training, attestations, discipline, documentation) and consistently implementing those procedures.

**Lancelot A. King is a counsel and Joseph Nardello is an associate in the Investment Management Group at Seward & Kissel LLP. Mr. King may be reached at king@sewkis.com or (202) 661-7196. Mr. Nardello may be reached at nardello@sewkis.com or (202) 661-7144.*