Hedge Fund Law Report
An Acuris company

Electronic Communications

Are Hedge Fund Managers Heeding the Message? Information Request List Provides Insight Into SEC Expectations on the Use of Electronic Communications by Advisers and Employees (Part Two of Three)

Dec. 7, 2017
By Kara Bingham, *Hedge Fund Law Report*

Investment advisers frequently use SEC document request lists to test their ability to efficiently produce documents that may be requested during an actual SEC examination. The SEC's Office of Compliance Inspections and Examinations (OCIE) periodically provides transparency into the adviser examination process by publicly releasing sample document request lists. Other times, redacted request lists are disseminated throughout the industry by examinees or third parties.

A document entitled "Information Request List" (Request List), purportedly being used by the SEC to request records in connection with adviser examinations focused on the use of electronic communications by advisers and their employees, has made its way into the public domain. While OCIE has not confirmed that this is an official request list being used, industry experts that routinely assist clients with SEC examinations agree that the substance and form of this Request List closely resemble those of information requests routinely sent by OCIE.

This second article in our three-part series explores the various components of the Request List and analyzes the implications and consequences of certain requests therein. The first article provided background on sweep exams, with particular focus on the putative electronic messaging examination and the potential drivers of SEC focus in this area. The third article will examine best practices for advisers when designing their electronic communications policies, taking into account the items requested in the Request List, as well as how advisers can proactively prepare for future scrutiny in this area.

For more on preparing for SEC examinations, see "Mock Audits Are Essential Preparatory Tools for Fund Principals in the Current Regulatory Environment" (Sep. 28, 2017); and "What Hedge Fund Managers Can Expect From SEC Remote Examinations (Part One of Two)" (May 2, 2016).

Breaking Down the Information Request List

The Request List follows a natural progression, explained Molly Yakubian, assistant vice president at Cordium. In responding to the Request List, an adviser would first have to

determine the electronic communication platforms that are being used by the adviser and its employees, and whether they fall within the scope of the request.

Once the adviser has an inventory of relevant electronic messaging platforms, Yakubian continued, it would then identify and provide the policies and procedures adopted by the adviser around those communications. The Request List then asks the adviser to disclose its recordkeeping practices in connection with electronic messages. Finally, the Request List seeks information related to the steps the adviser has taken to ensure that the information sent though electronic messaging platforms is protected and secure.

Defining Electronic Messaging

The scope of the Request List is limited to information surrounding "electronic messaging," which is defined to include:

> any and all forms of written communication conveyed electronically, including but not limited to instant messaging, text/SMS messaging, email, and personal or private messaging, whether conducted on the Adviser's systems or third-party applications or platforms, and whether sent using the Adviser's computers, the Adviser's mobile devices, or personally owned computers or mobile devices used by the Adviser's personnel (including independent contracts) for the Adviser's business, that are subject to the requirements of Rule 204-2(a)(7) or Rule 204-2(a)(11) under the Investment Advisers Act of 1940.

Notably, the Request List explicitly states that for purposes of this examination, advisers should exclude email messages that are sent or received using the adviser's email system and retained by the adviser, explained Chuck Daly, partner at Constellation Advisers.

What Communications Are Covered?

Examples of communication platforms that fall within this broad definition of electronic messaging include texting/SMS messaging; personal email accounts; Twitter; instant messaging systems; social media or networking websites; applications like Facebook and LinkedIn where users can post information and send and receive messages with other users; and private message applications such as WhatsApp and WeChat.

When you consider the variety of electronic messaging platforms that are potentially captured by this definition, "it appears that OCIE is zeroing in on a number of communication platforms that historically have not been specifically addressed in an adviser's electronic communications policy," noted Yakubian. These policies frequently include a blanket prohibition on employees sending or receiving business communications through any platform other than through the employee's business email account. In light of the exponential growth in communication channels, however, this approach may no longer be appropriate.

Additional Requested Information

After defining what constitutes electronic messaging, the Request List makes additional requests for descriptions of:

1. how an adviser and its associated persons use electronic messaging services or platforms, including what is and what is not permitted;
2. any divergences in the use of electronic messaging among different types of personnel or individuals in different positions at the adviser;
3. which devices are permitted or prohibited for use in electronic messaging; and
4. the specific types of electronic messaging conducted through each type of device.

"These specific requests suggest that the SEC wants to understand which electronic communications are being used by advisers for business purposes; how they are being used; and where and how advisers draw the line between permitted electronic communication platforms and prohibited ones," explained Yakubian.

In order to meet these requests, compliance officers must have a detailed understanding of how employees are using electronic messaging for business purposes and which devices are being used to send and receive electronic communications. There is a risk, however, that an adviser may not have a documented inventory of devices that employees are permitted to use to communicate electronic messages, or an ongoing process to track this information, noted Askari Foy, managing director at ACA Compliance Group and former Associate Director and Head of the National Technology Controls Program at OCIE.

"One way for an adviser to monitor the use of any new electronic communication platforms and devices by employees is through the use of periodic questionnaires and attestations," suggested Yakubian.

Compliance Program

The next section of the Request List seeks information surrounding the adviser's controls around electronic messaging platforms used by its employees. The following are specifically requested:

1. a copy of all written policies and procedures concerning the use of electronic messaging (or a description of any informal policies and procedures);
2. the identities of the individuals responsible for overseeing these policies and procedures, and a description of their responsibilities pertaining to electronic messaging;
3. a description of the adviser's processes for any ongoing monitoring and review of electronic messaging, as well as a description of how the adviser evidences that monitoring or review (including examples of any relevant exception reports, activity reports, etc.);
4. whether the adviser has detected any violations of its policies and procedures or any unauthorized use of electronic messaging, and the actions taken by the adviser;
5. summaries of any findings of internal audits or compliance reviews related to the adviser or its associated persons' use of electronic messaging, and copies of any reports documenting those reviews; and
6. copies of any risk assessments related to electronic messaging and how the adviser mitigates or addresses these risks, as well as any moderate- or high-risk findings relating to electronic messaging and any remediation efforts.

Potential Inadequacies With Adviser Compliance Programs

These detailed requests may lead to uncovering policy and procedure-related deficiencies during an examination. Certain private fund advisers may not have the resources and scale to have adequately documented policies and procedures addressing the numerous regulatory and security risk factors in the mobile environment, explained Foy. "Conversely, an adviser may be doing all of the right things from a functional perspective but may not have it in writing, or the adviser may have policies and procedures but not be implementing and following them."

Absent the inadequacies identified above, the next question is whether the adviser has policies and procedures that restrict certain types of devices from being used, and if so, whether the adviser has devised a way to monitor this going forward, Foy continued. "It is important that advisers adopt robust policies and procedures to clearly communicate to employees which devices may and may not be used for business electronic communications, and periodically test whether unapproved devices are being used or whether the information shared across these devices is being monitored."

For discussion of an enforcement action involving the unauthorized use of personal email accounts for business purposes, see "Business Emails Must Be Secure to Avoid SEC Enforcement Action" (May 12, 2016).

SEC Expectation May Exceed Adviser Act Requirements

One item to highlight for advisers, noted Yakubian, is the request around an adviser's monitoring and review of electronic messages. While the review of archived electronic communications is considered a best practice in the industry, neither the Investment Advisers Act of 1940 (Advisers Act) nor the rules promulgated thereunder specifically require an adviser to undertake this practice. "This request, however, strongly suggests that this is an expectation by the SEC," Yakubian observed.

See our three-part series on balancing the privacy rights of individuals against the adviser's obligations to monitor electronic communications: "How Can Hedge Fund Managers Reconcile Effective Monitoring of Electronic Communications With Employees' Privacy Rights?" (Apr. 4, 2014); "Three Best Practices for Reconciling the Often Conflicting Sources of Privacy Rights of Hedge Fund Manager Employees" (Apr. 11, 2014); and "Six Privacy-Related Topics to Be Covered by a Hedge Fund Manager's Compliance Policies and Procedures" (May 23, 2014).

See also "ECHR Decision Imposes New Criteria for Email Monitoring Practices on Fund Managers With European Operations" (Sep. 28, 2017).

Recordkeeping

"Where an adviser or its employees are using electronic messaging systems to communicate business information, those messages must be archived or maintained in some electronic storage form," explained Foy. If the messages cannot be automatically captured by an archiving solution, then employees should not be using those platforms or applications. "With that said, advisers may be able to come up with creative ways to retain that information. For example, perhaps there are third-party service providers that can assist with retention."

In light of the unambiguous requirement under Rule 204-2 of the Advisers Act (Books and Records Rule) to retain electronic messages that contain business information, it is not

surprising that the Request List makes several specific requests surrounding the adviser's recordkeeping practices, including:

1. whether the adviser maintains records of what devices and applications are being used for authorized electronic communications and by whom;
2. a description of how the adviser maintains required records relating to – or resulting from – electronic messaging, including how long and where those messages are stored;
3. confirmation of whether electronic messages are retained by a third-party vendor, and a description of the process for retention of those records by the vendor along with a copy of any agreements with that vendor; and
4. any written policies and procedures relating to the retention of electronic messaging.

Identifying Individuals May be Difficult

A significant risk underlying the SEC's focus on electronic communications is the identification of individuals using unapproved electronic messaging platforms, noted Sean McKeveny, consultant at ACA Compliance Group. This risk is particularly acute where there is no efficient archiving solution for the messages being sent and received through these applications.

"For example, private messaging applications like WeChat are commonly used for business purposes by bankers and traders in Asian trading markets, particularly China. This presents an issue for traders and portfolio managers of a U.S.-registered investment adviser who conduct business in those countries, as presently there is no effective technological solution for archiving WeChat messages due to encryption of the messages by the platform," McKeveny observed.

"There are means by which certain encrypted content can be archived," McKeveny continued, "but there are additional steps that have to be taken on the compliance side, the electronic-messaging-provider side and the employee side." When additional steps are added to the process, there is a risk that content may slip through the cracks. This is an issue that advisers are still trying to figure out.

Acceptable Use Policies May Help . . .

An adviser that has personnel conducting business in countries where individuals commonly use encrypted communication platforms for both personal and business purposes could consider adopting an "acceptable use policy," which would permit the adviser's employees to use specified communication platforms to engage in limited, non-business related communications with their foreign business contacts, explained McKeveny.

An acceptable use policy typically specifies the communication channels that may be used, as well as the purposes for which those channels may be used – for example, to communicate that the individual is running late to a meeting. Because the contents of the messages are outside the scope of the Books and Records Rule, the adviser would not capture those communications.

. . . But Risks Remain

"This is not an ideal solution, however, as the adviser runs the risk that once a communication channel is open, the employee or the person on the other side of the communication may send communications that rise to the level of being a business communication subject to retention under the Books and Records Rule," cautioned McKeveny. Even if the adviser trains the employee,

adopts an acceptable use policy and requires employees to periodically sign attestations that they have limited their use of these permitted communication platforms in accordance with the acceptable use policy, the adviser cannot control what the other party to the message writes in those messages. Furthermore, that third party may not be subject to the same books-and-records considerations as the adviser.

Use of Employer-Issued Devices

Another option to potentially reduce some of the risk of employees using unapproved communication platforms and applications is for the adviser to issue devices – for example, mobile phones, laptops, etc. – to its employees, accompanied by the adoption of a firm policy that restricts all business communications to adviser-issued devices. When the employer owns the device, it can wield much greater control over the applications that can be downloaded onto that device.

While restricting business communications to adviser-issued devices may reduce some of the risks discussed, the issue remains that all employees have their own devices, and if someone wants to take a conversation outside of monitored channels, he or she will find a way to do that, noted McKeveny.

Email Surveillance

"A better way to monitor for the use of unauthorized communication channels is through email surveillance that searches permitted electronic communications for indications that employees or third parties are moving, or trying to move, business communications to unauthorized platforms," McKeveny continued.

Examples of searches that advisers may want to employ during their reviews include:

- searching for names of the more popular platforms such as WeChat, WhatsApp, Gchat and any other platforms that are commonly used by the population in the local markets where the adviser does business; and
- risk-based phrases that may evidence the potential use of unapproved or unarchived communications, such as "check your phone" and "I sent you a text."

For more on the surveillance of electronic communications, see "Advertising Compliance Series: Six Methods for a Fund Manager to Test Its Advertising Review Procedures (Part Three of Three)" (Sep. 28, 2017); and "How Can Hedge Fund Managers Structure, Implement and Enforce Information Barriers to Mitigate Insider Trading Risk Without Impairing Securities Trading? (Part Four of Four)" (Feb. 6, 2014).

Security and Privacy of Information

The last category of information requested relates to the security and privacy of information being transmitted through electronic messaging platforms, including:

1. any written policies and procedures, or a description of any unwritten policies and procedures, addressing the transmittal of sensitive information (*e.g.*, non-public information, personal client information, etc.) in electronic messaging;

2. any written policies and procedures, or a description of any unwritten policies and procedures, addressing security measures/precautions that the adviser takes to ensure the security of sensitive information through the use of electronic messaging; and
3. a description of any known breaches in securing information contained in electronic messaging, as well as any actions taken by the adviser with respect to those breaches.

These requests underscore the high priority that the SEC places on the protection of customer data by advisers. Stephanie Avakian, the SEC's Co-Director for the Division of Enforcement, previously stated that when it comes to cybersecurity and protecting client information, one of the SEC's enforcement buckets includes cases where advisers have failed to take appropriate steps to safeguard information in compliance with rules like Regulation S-P.

It stands to reason, therefore, that it is not enough for an adviser to ensure that sensitive information that is stored on its own servers is secure. Rather, advisers also need to evaluate the security of data when transferring information through electronic means.

See "SEC Tackles Internal Cybersecurity Issues While Sharpening Cybersecurity Enforcement Focus" (Oct. 5, 2017).

The SEC expects advisers to have policies and procedures identifying the type of information that may and may not by communicated through certain electronic messaging platforms, explained Foy. Without these policies, there is a risk that advisers may not have made a determination prior to sending information whether that information is critical or sensitive. Before advisers can classify information, however, they must first define what is and is not material.

See "Failure to Safeguard Customer Data, Preserve Records and Properly Supervise May Expose Broker-Dealers to FINRA Enforcement Action" (Dec. 1, 2016); "In Deutsche Bank Case, SEC Emphasizes Protecting Information From More Than Just Cyber Threats" (Nov. 10, 2016); and "SEC Enforcement Action Illustrates Focus on Investment Adviser Obligation to Secure Client Information" (Jun. 23, 2016).