HEDGE FUND
legal & compliance digest

www.hedgefundlcd.com April 20, 2017

How Hedge Fund Managers Can Mitigate the Risks Associated with Employees Communicating Through Messaging Applications

Supervising emails and other business communications has extended beyond the firm's server for hedge fund managers' whose employees frequently communicate, for both personal and business purposes, through text and messaging applications on their mobile devices. While employees can access the firm's communication networks through SMS text messaging, webmail or proprietary instant message applications on company-issued or personal mobile devices, the devices also offer access to third-party instant message applications, such as iMessage, Snapchat and WhatsApp, whose communications may not be captured by firms' servers. An inability to control or supervise employees' text and messaging application activity—since they may reside on servers external to the manager—can present additional regulatory risks for registered managers required by recordkeeping rules to retain and archive such communications related to the business.

This article reviews the recordkeeping requirements that apply to private fund managers' employees' use of texting and messaging applications; assesses the risks posed by uses of messaging apps that circumvent a firm's infrastructure to document and record such communications; and discusses technology solutions to capture such messages and the best practices, policies and procedures designed to effectively address the risks presented.

Recordkeeping Requirements

As registered investment advisers with the Securities and Exchange Commission, hedge fund managers must comply with certain recordkeeping requirements that govern the use of text messaging by employees.

Investment Advisers Act Rule 204-2 sets forth the specific mandate that advisers must make and keep true, current and accurate books and records related to their advisory business. Rule 204-2(e) requires that the records be maintained "in an easily accessible place for a period of not less than five years, the first two years in an appropriate office of the investment adviser." Rule 204-2(g) details rules for retention, non-rewritable storage and ease of retrieval and viewing. In addition, Rule 17a-4 of the Exchange Act requires firms to archive electronic business communications in non-rewriteable and non-erasable formats for at least three years.

The recordkeeping rules are straightforward enough, but how they apply to the realities of messaging practices may be more complicated. According to Holly Weiss, a partner at Schulte Roth & Zabel, "A threshold question for an employer is whether it is obligated to retain records of employee text messages or other mobile communications. If an employer is required to retain records of all business-related communications, it should not be liable for not maintaining text messages on personal devices if the employer prohibits employees from using these modes of communication for business purposes. Most hedge fund managers have books and records obligations under Rule 204-2 of the Investment Advisors Act. Because of this, they typically maintain copies of all electronic records for at least six years, even though only a subset of such records is required to be retained for that long. It's too cumbersome to separate out the records, and there also are interpretive issues as to exactly what is required to be maintained. For managers following this typical approach, they should require that all business communications be on the firm's systems."

The recordkeeping rule requires managers to make their books and records available for review, added Gregory Nowak, a partner at Pepper Hamilton. "If the manager doesn't properly enforce those rules by maintaining tabs on what its employees are doing and what systems they are using to communicate and retaining those records, then it becomes the fault of the manager. Any way in which an employee communicates about work-related matters has to be captured. People have always tried to skate around the rules if they can. Unfortunately, if you do that and the SEC finds it, you're going to have a problem."

Ted Eichenlaub, a partner at ACA Compliance Group, noted that when it comes to electronic communications such as text messages and other third-party messaging apps, the Advisers Act is "a bit grey at this point." He continued, "The SEC has been trying to overhaul the Advisers Act for many years, most notably the books and recordkeeping rule. Paragraph seven of that rule outlines written communications that are required to be maintained, and it is old and antiquated and doesn't reflect electronic communications. The SEC has been suggesting that they would overhaul this rule, but they haven't yet. Some of the communications—whether they're emails, texts or social media—it's a grey area as to what has to be maintained and what doesn't. If the SEC comes into a firm and they know people at the firm have been using these various types of communications, then they will certainly ask for access to these platforms and ask to see a sampling of records of these communications. The SEC has put out guidance through the exam program about various social media they will review but the actual rules just haven't caught up with these positions."

FINRA also has recordkeeping requirements related to text messaging and other electronic communications that private fund managers under its supervision must follow. "FINRA will review firms' compliance with their supervisory and record-retention obligations with respect to social media and other electronic communications in light of the increasingly important role they play in the securities business. We note that these obligations apply to business communications irrespective of the medium or device used to communicate. Under SEC and FINRA record-retention requirements, firms must ensure the capture of business-related communications regardless of the devices or networks used. A firm must capture and maintain all business-related communications in such a way that the firm can review them for inappropriate business conduct," the self-regulatory organization said in its 2017 Regulatory and Examination Priorities Letter.

Additionally, FINRA Rules 3110 and 3120 require firms to establish, maintain and enforce supervisory systems and written supervisory procedures reasonably designed to comply with their recordkeeping obligations. Firms are also required to periodically review and update their recordkeeping written supervisory procedures and to have appropriate written supervisory control procedures to test and verify that those recordkeeping supervisory procedures are reasonably designed to comply with applicable recordkeeping laws and regulations and FINRA rules, and to update or amend them if necessary. FINRA Rule 3310 states that firms must be able to readily produce data from corporate emails, texts, instant messages, and now even web content, from their social media communication channels.

According to Michael Pagani, senior director of product marketing and chief evangelist at Smarsh, "There is a particular paragraph in the FINRA priorities letter for 2017 that is pertinent to record-retention requirements. This is the first year we've seen FINRA spell out 'social media and other electronic communications,' and we've seen past guidance refer to email when it comes to records retention. You need to capture business communications regardless of the devices or networks used."

Recordkeeping violations resulting from texting or other messaging applications increasingly are cited in regulatory examinations. According to Eichenlaub, "This is absolutely coming up in exams. The SEC has litigated against firms regarding texting. It's particularly problematic given that technology moves at the speed of light, and just when the compliance officer or the chief technology officer thinks they have everything covered, something new will come out. There is not a foolproof solution that would limit or essentially eliminate all of the absolute risks associated with various messaging apps and communication devices."

In April 2016, for example, the SEC entered into a settlement with New York registered broker-dealer Craig Scott Capital, and CSC's co-founders and principals, Craig Taddonio and Brent Porges, Taddino and Porges were

censured for using non-CSC and personal email addresses for receiving faxes that included sensitive customer records and information, and for corresponding about firm business, in violation of Regulation S-P, Rule 17a-4 and CSC's own written policies and procedures. The SEC also found CSC's written supervisory procedures inadequate because they were not tailored to the firm's actual practices, among other reasons.

Implications of Violating Recordkeeping Rules
The typical legal and regulatory consequences for managers who fail to produce records of text and other messaging application communications include fines and other disciplinary action against the firm and the person(s) involved.

According to Nowak, "If the manager doesn't deliver the required records, then the SEC or other regulator can fine the manager, censure the manager, ban the manager or bring enforcement actions. They can also go after the individuals involved and sanction them and subject them to special supervisory procedures."

Technology

There are both legitimate and illegitimate uses of texts or other messaging apps for business purposes. Pagani observed that people who rely on these messaging services and other new apps tend to be younger employees who are comfortable with the latest apps and firms using new apps in campaigns to reach millennials in order to promote their businesses.

Eichenlaub noted, "I don't think it's necessarily that an employee wants to perpetrate a crime as much as it's because the people coming into the industry are just used to using certain applications that may not be widespread in the industry just yet."

Certain texting applications can provide more recordkeeping and retention issues than others. Pagani pointed to a program called Confide, which enables users to send messages that are deleted as soon as they are read. "It also blocks the ability to take a screen capture. That's a big problem. There's no way to archive these communications."

iMessage also presents problems for managers, Pagani said, "Because it is encrypted and no vendor can archive those messages. It is a sealed communications method. It is an app using the data network and is encrypted. We encourage firms to use a carrier-based texting program so they can be captured and archived." Perhaps surprisingly, Eichenlaub noted that Dropbox is one of the communication channels that has been recognized as requiring a bit of additional oversight.

As new software that employees could use to communicate with clients or industry insiders constantly becomes available, firms must either ban the use of these apps or find ways to capture communications within them.

According to Pagani, "You have to fight technology with technology. You need to first establish your policies and make sure they mirror the regulators' requirements. You can then see what technology solutions are available that allow you to automate the review process and look for communications that violate your policies."

Using iMessage text messaging as an example, Pagani said, "There is a program called the Device Enrollment Program that enables you to grab the messages. You can also manage the devices and turn off iMessage. With the DEP program for companies, you can have one Apple ID for the organization and centrally control which applications can be installed on the phones."

Firms also have to recognize who is responsible for oversight of employees' use of various messaging programs. According to Nowak, "Oversight has to be a joint effort between your technology folks and your compliance folks. The compliance people need to be involved, because they need to evaluate the implications for the firm. The tech people need to be involved, because they are the ones who understand how these programs work and how they could potentially hurt the firm."

Eichenlaub agreed that oversight should be a joint effort between compliance and technology. "First, the government overall has been focusing on cyber and IT risks, and the SEC has been taking up in their examination program these risks and some related issues. This has elevated the discussion and forced chief compliance officers and general counsels to really stay attuned to what's going on in this space. In order to stay on top of these issues, they have developed much closer partnerships

between the chief compliance officer, the general counsel and the IT department. I think there has been a recognition in the industry that IT is no longer just about disaster recovery but looking at cybersecurity and various electronic communications and how various systems are being used within a firm. They have to think about what the approval process is for different systems, who has access rights and how they are administered. This helps the CCO and the general counsel become aware of all of the different platforms that are available for employees to use these days and the risks they present."

Managers' oversight of applications and ability to retain records change if the mobile device is owned by the employee rather than the firm, said Weiss. "Company-owned devices, and the business data stored on those devices, can readily be secured by the company. A device owned by the employee that contains personal information may not readily be secured legally. For example, employees have successfully sued their employers under the Computer Fraud and Abuse Act for accessing their personal devices without authorization. Monitoring communications on a personal device may also raise issues under the Electronic Communications Privacy Act. Mobile management software can be used to segregate firm information from personal information, and, therefore, can go a long way to avoiding privacy concerns, while enabling managers to retain control over and access to firm-related information."

Pagani explained certain supervisory steps and programs designed for recordkeeping compliance on company-issued phones. "For personal devices, you can use containerization to set up a secure environment on the personal devices for the business. It is basically an app that you open and authenticate through. All of the messages sent through this containerized app are being archived. It's a way of creating a secure compliance work environment on a personally-owned phone. Employees using their own personal phones would have to sign off on this and acknowledge that if they are doing anything related to firm business, it will be done through the secure work environment. Any work done outside of this environment is on the employee, and they assume liability."

Eichenlaub added, "Obviously the firm has control over its company-issued mobile devices but, like I said before, firms can't control a rogue person. If someone wants to communicate in an unapproved platform for business use, they will do it. That's why we try to focus on a policy that conveys to employees they won't use personal devices, personal emails, chats or texts for business use. That's what you have to do in order to protect the firm. The employees have to take some responsibility for their actions, so if they go rogue, that liability is going to be on them, and it won't be because the firm's policies and procedures were not adequate. Employees need to sign off on the fact that they are going to comply with these policies and procedures, and if they go against them, it will be their own doing and responsibility. That's the harsh reality of it."

Policies and Procedures

To have an effective supervisory system, firms must establish clear policies and procedures regarding the use and supervision of electronic communications, which must be updated to incorporate new technologies. Firms also need to make sure employees have access to these policies and procedures, which should contain a list of permissible electronic communication mechanisms and an explanation of the potential consequences of non-compliance with these policies and procedures.

According to Eichenlaub, "Our standard recommendation to all managers is to acknowledge the fact that there are vendors and avenues outside of the firm's approved vendors that employees may use. By policy, we recommend managers prohibit the use of anything other than approved communications methods and train employees on those, and have employees sign off that they will not use unapproved communication methods for business. We recognize it's not foolproof, but it is certainly a best practice."

Weiss explained, "Fund managers generally prohibit their employees from using means of communication that the fund manager cannot secure and retain. Otherwise, fund managers may not be well-positioned to discover and take action with respect to misconduct relating to the business, to conduct investigations or to comply with discovery and books and records obligations."

Nowak said, "If the manager simply doesn't have proper policies and procedures in place, any violations are on the manager. However, if

there are policies in place, and the manager has a robust compliance program that employees were made aware of, but still act inappropriately, then the violation falls to the employee."

"Policies are designed to give the firm the ability to say to regulators that there is a policy, the employees signed off on it and said they would follow it, they didn't follow it and they have been fired," Nowak continued. "This could allow the firm to continue without being fined itself for the actions of a rogue employee. A lot of employees don't realize that policies like this are designed to make it possible for the firm to survive an investigation by allowing the malefactor to be cut off. "

As explained above, in designing policies and procedures, managers need to list the approved messaging programs that employees can use. When determining whether to approve the use of certain new messaging apps, Eichenlaub advised, "As a chief compliance officer you want to facilitate business, and you don't always want to say no, but I think there are some areas where you just have to. In evaluating a program or messaging platform that doesn't facilitate the archival of those messages or the surveillance of those messages, I think a firm needs to strongly consider the value of letting employees use that program. As a chief compliance officer, I would think that letting employees use a messaging program that I couldn't surveil or archive and review later, that would be a major risk area for me and would be something that I wouldn't allow, because I would have no way of knowing what's being communicated over that system. That would be problematic."

In addition to policies and procedures, managers may also have employees sign an attestation that they have read, understood and will comply with the firm's policies and procedures. According to Weiss, "The fund manager's policies—including prohibitions on certain modes of communication for business purposes—are the first step. Fund managers should ensure that their employees know about the policies, understand them and know how to comply with them. This is where training can be very helpful. If a fund manager has reason to believe an employee is breaking the rules—as with any other misconduct—the fund manager should investigate and take appropriate remedial action. Regular affirmations concerning compliance with firm policies are common."

"Every employee has to sign off on a code of ethics every year so there is already a mechanism in place," Nowak said of the attestations. "I recommend to managers that they piggyback their cybersecurity and their personal device policies onto those periodic certifications. This way you are reminding people at the same time of all the things they cannot do and what the rules are."

Employees also should be trained on mobile communications and record retention requirements. As Weiss advised, "Training for all employees in certain areas related to mobile communications is a good idea. The starting point is usually the employer's policies, and the training is geared to ensuring that employees know about, understand and comply with them. Topical areas include: prohibitions on particular means of communication for business purposes (and permitted modes, such as the firm's systems), reporting requirements for lost or stolen devices, rules relating to cloud-based storage, use of unsecured wireless networks, rules regarding downloading and uploading information and software, and password security. Live, interactive training is effective. However, regular messaging to employees regarding particular matters is also helpful."

Added Eichenlaub, "Good business and good compliance programs dictate that employees should be trained. This training should be done at least annually and for new employees covering the firm's compliance program. You can do specialized training on those aspects that only pertain to certain employees. As for determining who needs to be trained and what the training should cover, the size of the firm matters. We advocate all employees are trained in some manner on the employee-related compliance issues that apply to everyone, such as personal trading and communicating with clients, co-workers and industry experts."

Nowak summarized, "You need to educate your employees. They need to understand the consequences of violations of these rules. They have to understand that if they violate the rules intentionally, it could very well mean their job. They could be fired if they intentionally do something that is inappropriate."