Hedge Fund Law Report
An Acuris company

Electronic Communications

How to Avoid Five Common Duty to Supervise Traps: Conduct Proper Trade and Electronic Communications Surveillance (Part Two of Three)

Sep. 13, 2018

By Robin L. Barton, *Hedge Fund Law Report*

The essence of a duty to supervise violation is that the broker-dealer or investment adviser was not sufficiently monitoring its employees to ensure that they were not violating any of its policies and procedures or any securities laws. Pursuing failure to supervise claims therefore enables the SEC to attack an adviser's or a broker-dealer's lax or inadequate compliance program. In addition, failure to supervise charges are attractive to the SEC because they only require proof of negligence.

An examination of a sampling of recent SEC enforcement actions alleging failures to supervise revealed similar mistakes made by the relevant broker-dealers or investment advisers. With the circumstances of these enforcement actions as the backdrop, the second and third articles in this three-part series discuss five common duty to supervise traps. This second article analyzes failure to conduct adequate trade surveillance and communications surveillance. The third article will explore failure to respond properly to red flags; implement reasonable policies and procedures; and properly train supervisors, traders and salespeople. The first article in the series reviewed the duty to supervise for both broker-dealers and investment advisers and summarized the duty to supervise violations in these enforcement actions.

See "Five Steps That CCOs Can Take to Avoid Supervisory Liability, and Other Hedge Fund Manager CCO Best Practices" (Mar. 27, 2015).

Trap #1: Poor Trade Surveillance

In the enforcement action against Deutsche Bank Securities Inc. (Deutsche Bank), the respondents conducted surveillance of trades, but their surveillance was not properly calibrated for the trading activity or was ineffective in that it did not flag questionable trades. For example, the trades in question in the Deutsche Bank case involved secondary market transactions in non-agency commercial mortgage-backed securities (CMBS). In its trade surveillance, however, Deutsche Bank used generic price deviation thresholds to flag potentially suspicious trades instead of ones tailored to these specific securities.

See "For Hedge Funds, Ownership of Commercial Mortgage-Backed Securities Servicers Offers a Growing, Uncorrelated Stream of Fee Income and Advantageous Access to Distressed Mortgages, but Not Without Legal and Business Risk" (Sep. 24, 2009).

In the Morgan Stanley Smith Barney LLC (Morgan Stanley) action, Morgan Stanley allowed its "financial advisers" to initiate third-party wires of up to $100,000 per day per client account based on the financial adviser's attestation of having received a verbal request from the client. Although the firm used fraud detection software to monitor wire transfers and trigger alerts if certain thresholds were exceeded, the software was not "reasonably calibrated to analyze risks" created by this practice. As a result, the software failed to flag any of the more than 50 unauthorized third-party wires one financial adviser initiated by falsely representing that he had received a verbal client request.

"One would expect to see these sorts of errors at non-institutional environments where they may not have robust surveillance systems or personnel dedicated to monitoring for this sort of behavior," remarked Emma Rodriguez-Ayala, partner at Faegre Baker Daniels and former in-house counsel for an SEC-registered investment adviser.

"A compliance program should be reasonably designed to ensure compliance for the firm's business. People always focus on the 'reasonably designed' element, adopting programs that they believe are the basic 'market standard' or are reasonable compared to others. They almost always forget the second part: 'for the firm's business,'" observed Rodriguez-Ayala. "The compliance program

really needs to be tailored to the firm's business environment, taking into account what the firm is doing; how the firm is doing it; who the employees are; and what incentives employees have internally to behave in particular ways."

See "Hedge Fund Manager Deerfield Fined $4.7 Million for Failing to Adopt Insider Trading Compliance Policies Tailored to the Firm's Specific Risks" (Sep. 21, 2017).

"The issue is that firms may build a compliance program by buying, renting or licensing really great compliance software but then don't tailor it for the business, or they hire compliance professionals who really know compliance and regulations but don't understand the firm's underlying operations and strategies," noted Rodriguez-Ayala. She identified what she believes is the underlying concern in all of these enforcement actions: "The firms had compliance systems that were valid on their face but did not seem to take into account the underlying business, the existing incentives for misconduct and how the operational infrastructure could be manipulated to allow for misconduct."

As to trade surveillance specifically, Rodriguez-Ayala warned that although software is incredibly helpful for systematically tracking what employees are doing for the funds, their personal accounts and the management entity, there still needs to be a human component. "Software works off of trigger words, rules or baselines that should be set for the system based on the firm's business," she explained. "When the software does raise flags, someone needs to examine those flagged trades individually but also needs to look for patterns – such as a seemingly immaterial flag that keeps getting raised periodically for the same employee or business unit – and for gaps in policies."

For instance, as described in the Morgan Stanley enforcement action, Rodriguez-Ayala pointed out that the financial adviser was able to steal money from client accounts in $100,000 chunks because he could say he had verbal approval from the client, a practice that was permitted under the firm's policy. "The problem is that nobody looked at the pattern created by these transactions. No one checked to see if someone was using an appropriate policy – *i.e.*, moving $100,000 from client accounts based on verbal instructions – to behave inappropriately – *i.e.*, moving that money into the employee's personal account," she noted.

The lesson is that effective trade surveillance must be tailored to the kinds of trading the adviser or broker-dealer engages in – and the risks posed by that trading – and cannot simply rely on software alone.

See "Cordium and Aite Group Survey Benchmarks Use of 'Regtech' by Asset Management Firms" (Feb. 8, 2018); and "How Hedge Fund Managers Can Use Technology to Enhance Their Compliance Programs" (Nov. 17, 2011).

Trap #2: Poor Communications Surveillance

Poor surveillance of employees' communications – most notably emails – was also a common thread in some of the enforcement actions. For example, Deutsche Bank's communications surveillance did not sufficiently incorporate search terms unique to the CMBS market and its particular risks for misconduct. As a result, its surveillance system did not flag any of the suspicious communications.

Similarly, in the enforcement action against Merrill Lynch, Pierce, Fenner & Smith Inc. (Merrill Lynch), the SEC highlighted several flaws in Merrill Lynch's surveillance of electronic communications:

- It did not have sufficient personnel engaged in communications surveillance. A team of six to nine individuals was tasked with reviewing the communications of about 10,000 employees spread across 70-80 groups. Each day, the team reviewed a sample of about one percent of each group's communications, usually one or two days after the date of those communications.
- The reviews themselves were limited to determining whether each individual communication reflected a potential violation of firm policy rather than determining whether a communication, when considered together with other communications related to the same transaction, reflected a potential false or misleading statement related to that transaction. As a result, Merrill Lynch's surveillance systems never detected any of the false or misleading statements at issue.
- Because of the "opacity of the market" for non-agency residential mortgage-backed securities (RMBS), there was a "heightened risk" that Merrill Lynch personnel could engage in fraudulent sales activities. In light of that risk level, the firm needed surveillance procedures reasonably designed to detect false or misleading statements related to that market.

Targeted Surveillance

As with trade surveillance, communications surveillance should be geared to the risks specific to the firm's trading activity and markets, said Sean McKeveny, principal consultant with ACA Compliance Group. To ensure these searches are effective and appropriately targeted, he observed that compliance must have "an intimate knowledge of what trading activity looks like, and what sort of dialogue is standard and what would be outside the norm." Rodriguez-Ayala agreed, adding that "if compliance does not understand the actual business, individuals who want to do something bad can easily do it."

To aid in targeting communications surveillance, firms should create a tailored lexicon of key words and phrases, advised McKeveny. He noted, however, that the lexicon should be "a living document" which is periodically revised to add new terms and eliminate those that are not returning meaningful results. "Firms need to balance having a well-established concrete framework for communications surveillance with recognizing the need for the components of that framework to evolve," he observed.

In addition, compliance must also "understand that certain search terms may be more relevant for certain subsets of groups within the firm. If compliance establishes an extremely expansive lexicon and applies it across a broad group, it is going to get a bunch of noise," noted McKeveny. "Key issues that might be present in the correspondence of certain individuals may be overlooked because of the sheer volume and noise that the other results are generating."

To combat that problem, McKeveny recommended that compliance use a "well-established archival system to group certain individuals based on their various risk categories and then apply search terms specific to their roles or the investments that they are making."

That being said, McKeveny clarified that certain aspects of communications surveillance will apply universally to all employees regardless of role or responsibility. For example, data being sent outside the firm or to employees' personal email accounts, as well as phrases such as "keep this confidential," "please do not forward" and "for your eyes only" are generic red flags that compliance should look for in all communications, he advised.

The software or systems being used to monitor and archive communications are important for another reason.

"Compliance personnel should really understand the intricacies of an archival system because they can use tools such as Boolean logic to white list or weed out false positive results," said McKeveny. "Connectors like 'AND,' 'OR' and 'NOT'; wild card characters (*,~,!); and the directional flow of messages should all be considered when building searches. In my opinion, it is better to get a smaller volume of targeted results than a large volume of results that may mostly contain just noise."

In addition to "standard" search terms, compliance should gather supplementary information for the applicable period of communications being reviewed, recommended McKeveny. "If I am reviewing communications for July, I would want information on the trading activity during that month; any particularly profitable transactions that took place; new relationships that came into the firm; new and terminated employees; etc. and then use that information to tailor the reviews," he explained.

Human Element

"Communications surveillance is challenging because it isn't just email – it is also chats, texts, voice mail, Bloomberg, etc.," observed Rodriguez-Ayala. "Software and automated searches are useful for taking a first pass at communications and flagging potentially questionable exchanges, but they cannot replace the human element."

While acknowledging that certain communications surveillance can be automated, McKeveny also warned that "much of the review requires a human eye. I do not think there will ever be robots that can make the determination that an email is problematic." Still, smart use of automated searches can ensure the most effective use of the staff reviewing communications, he noted.

The human component of communications surveillance is interpretation – *i.e.*, trying to figure out what is happening in these exchanges, explained Rodriguez-Ayala. Compliance must overcome several obstacles to effectively interpret communications.

The first challenge is the sheer volume of communications. "It is an overwhelming process for compliance professionals to conduct surveillance if it is not done in a way that is very thoughtful and systematic," remarked Rodriguez-Ayala. Firms can use targeted software searches to narrow the number of communications to be reviewed and focus the efforts of the staff, she said, but they still need to have a sufficient number of individuals involved in these reviews. She expressed surprise that Merrill Lynch allegedly had merely six to nine people conducting email surveillance on 10,000 employees and observed, "That ratio is really low."

"Throwing more people at the problem is not the solution, however," warned Rodriguez-Ayala, who added that it is important to assign communications review to individuals who will be able to accurately interpret the communications. "If you dump a million emails on junior employees, they are unlikely to recognize the flags, trigger words and context of the communications," she explained. "A lot of firms outsource email surveillance, but again, those outsiders may not have the business context for what they are reading."

When Rodriguez-Ayala served as in-house counsel, the whole legal and compliance team reviewed emails, but the emails were assigned to employees based on critical roles. For example, she explained that more junior compliance people were assigned to review the communications of more junior or lower risk employees, while the communications of higher risk employees were reviewed by senior compliance personnel.

In addition, advisers and broker-dealers should consider involving supervisors for targeted communications surveillance of the employees whom they supervise.

"For some firms, such as a direct trading manager, it absolutely makes sense for supervisors to be involved," said Rodriguez-Ayala. "Their involvement, however, should be very focused as to what they are reviewing. Supervisors should not be conducting general reviews."

For example, as a remedial step in response to the violations, Merrill Lynch now requires the RMBS desk supervisor to periodically review several days' of electronic communications of each RMBS desk employee for potential false or misleading statements.

Another challenge is conducting communications surveillance in a way that considers a series of exchanges or an email stream and puts the pieces together to create the whole picture, observed Rodriguez-Ayala. One solution she recommended was to use technology to ensure that connected emails go to the same reviewer.

For instance, another remedial step Merrill Lynch took was to create an electronic communications monitoring tool that compiles all communications related to a trade in which the markup exceeds a certain percentage.

Also, Rodriguez-Ayala advised holding regular meetings to discuss the results of communications reviews and possibly identify connections that might otherwise be missed. "We had a situation where someone raised a hand at one of these meetings and mentioned seeing something 'weird' in an email," she recalled. "It turned out that three other people noticed the same thing in emails from different employees. That sort of collaborative approach to tackling email surveillance was very helpful for us."

For more on SEC scrutiny of electronic communications, see our three-part series: "SEC Takes Steps to Drill Down on Electronic Communications" (Nov. 30, 2017); "Information Request List Provides Insight Into SEC Expectations on the Use of Electronic Communications by Advisers and Employees" (Dec. 7, 2017); and "Six Key Issues to Address in Electronic Communication Policies and Guidance on Preparing for Future Scrutiny of Electronic Messaging" (Dec. 14, 2017).

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL