Regulatory Perspectives by Theta Lake

Enforcement Lessons From FINRA's Focus on Communications Compliance

Published Jan 19th 2023 by
Susannah Hammond, Theta Lake

The last quarter of 2022 highlighted the Financial Industry Regulatory Authority's (FINRA's) continuing regulatory focus on communications compliance with a series of disciplinary actions.

At a Glance

Part of FINRA's mission to protect investors and safeguard market integrity in a manner that facilitates vibrant capital markets is the clearly stated expectation that firms learn the lessons from enforcement action. There are 4 recent enforcement actions highlighting a range of lessons for firms which would be well advised to undertake a comprehensive and wide-ranging review of the following:

- Written supervisory procedures (WSPs) - with regard to the capture and oversight of electronic communications. Specifically, firms should consider a gap analysis to ensure that the WSPs clearly identify the personnel responsible for searching or reviewing electronic communications, state how frequently reviews should occur, and provide any information about the sample size for review.
- Communications records management policy and procedures - to ensure there is a centralized list/database of what data is held where with the ability to undertake a comprehensive search across records.
- Compliance monitoring program - to ensure that all policies, processes, procedures, as well as prohibitions (such as the use of unapproved email accounts and the transmittal of blank or incomplete documents to customers) are adequately covered.
- Approach to communications surveillance - in particular, to ensure that any communications flagged for review are completed and also have the attachments examined.

Enforcement 1

A broker was found to have failed to establish, maintain, and enforce a reasonable supervisory system, including WSPs, to review electronic communications that its registered representatives sent and received. As a result, in December 2022 the firm was censured and fined $45,000. The firm was also mandated to undertake remedial action, certified by an executive, which required a retrospective review of emails sent and received during a five year period to detect any FINRA rule violations.

Relevant Regulatory Requirements

FINRA Rule 3110(b)(4) requires every firm's written supervisory procedures (WSPs) to "include procedures for the review of incoming and outgoing written (including electronic) correspondence. . . ." Such procedures "must be appropriate for the member's business, size, structure, and customers."

Rule 3110(b)(4) also requires that "reviews of correspondence . . . must be conducted by a registered principal and must be evidenced in writing, either electronically or on paper."

As discussed in FINRA Regulatory Notice 07-59, member firms may employ risk-based procedures to review electronic communications so long as they reasonably consider how to effectively flag potentially problematic communications, including the use of keyword-based reviews, random sampling, or both.

Key Lessons:

Firms would be well advised to undertake a comprehensive and wide-ranging review of their WSPs with regard to the capture and oversight of electronic communications. Specifically firms should consider a gap analysis to ensure that the WSPs:

- Clearly identify the personnel responsible for searching or reviewing electronic communications, state how frequently reviews should occur, and provide any information about the sample size for email review.
- Specify any keywords or process for identifying keywords to flag electronic communications for review. In practice, the use of AI for identifying risks will overcome many of the challenges of rigid, lexicon based approaches enabling communications to be understood in context and reducing the number of false positives.
- Describe any parameters for conducting random sampling. Firms need to be able to justify sample sizes as reasonable and have a regular review of the approach and assumptions made. Approaches and technology which enable risks to be automatically flagged will allow compliance teams to prioritize their review of the highest risks, whilst reviewing a sample of others.

- Describe any types of red flags or issues that would require follow up steps from reviewers or any steps for escalating issues identified during email review. Firms should also ensure that there are processes in place to oversee and maintain an audit trail of the review of all communications identified in the random sampling.

Enforcement 2

A broker was found to, from May 2017 to March 2021, have failed to timely or completely produce certain phone records in response to requests in ten separate FINRA investigations. In certain responses, the firm also inaccurately represented to FINRA that phone records older than 18 months were not available, even though that was not the case. The firm did not promptly alert FINRA once it learned of its production failures. As a result, in December 2022, the firm was censured, fined $1.1m and required to undertake remedial action.

Relevant Regulatory Requirements

FINRA Rule 8210(a)(1) requires member firms "to provide information orally, in writing, or electronically . . . with respect to any matter involved in the investigation, complaint, examination, or proceeding."

Rule 8210(a)(2) requires member firms to permit the inspection and copying of the member's books and records with respect to any matter involved in the investigation, complaint, examination, or proceeding.

Rule 8210(c) provides that "[n]o member or person shall fail to provide information … or to permit an inspection and copying of books, records, or accounts pursuant to this Rule."

Key Lessons:

It is a core competency for firms to be able to respond promptly and accurately to regulatory requests for information. A key feature of that competency is comprehensive records management so that the compliance function has a clear and complete line of sight to what records are held where and under what deletion criteria.

- Firms would be well advised to undertake a review of their records management policy and procedures and ensure there is a centralized list/database of what data is held where. Even if data is simply being held for use with an analytics tool for business planning and not retention or production purposes, it still may have relevant records for regulatory purposes.
- If a firm has a purge protocol in place it must have an exception built in so that any records subject to a regulatory request are kept and not deleted. Inherent in that

approach is the ability to act swiftly once a regulatory request has been received making it crucial that firms can comprehensively search and retrieve all relevant records.

- No regulator has any tolerance for being misled and that intolerance is even greater when the regulator requires information for its investigations into allegations of potential misconduct, including unauthorized trading, discretionary trading, and excessive trading. As soon as a firm becomes aware that it has given inaccurate or incomplete information in response to a regulatory request it must inform the regulator immediately.

Enforcement 3

A **compliance officer** was found to have failed to reasonably supervise the sales practices of two registered representatives. The first breach was a failure to reasonably supervise recommendations made by Representative A. The second breach was a failure to reasonably investigate red flags that Representative B was using an external email address to transmit securities-related documents to the firm's customers, or ensure those communications were retained. As a result, in December 2022, the compliance officer was subject to a 40 business-day suspension from associating with any FINRA member in all principal capacities and fined $5,000.

Relevant Regulatory Requirements

FINRA Rule 3110(a) requires members to establish and maintain a system to supervise the activities of associated persons that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA Rules.

FINRA Rule 3110(b) requires members to establish, maintain, and enforce written procedures to supervise the types of business in which it engages and to supervise the activities of associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations, and with the applicable FINRA Rules. The duty to supervise under Rule 3110 also includes the responsibility to ensure recommended transactions are suitable, and to reasonably investigate red flags that suggest misconduct may be occurring and to act upon the results of such investigation.

Key Lessons

Any systems and controls infrastructure should have a means by which red flags or other warnings of possible policy breaches can be raised and investigated. Any red flags raised should, as a matter of course, be reviewed and results of investigations documented. Undue

numbers of false positives can be used to refine the criteria by which red flags are raised in the first instance.

In terms of the supervisory review process:

- Firms would be well advised to review their WSPs and ensure that the policies, processes and procedures are accurately reflected in the associated compliance monitoring program to ensure that all prohibitions (such as the use of unapproved email accounts and the transmittal of blank or incomplete documents to customers) are adequately covered
- Where heightened supervision of any kind is required, firms should have the means to not only review but also be alerted to and ensure the retention of any related communications. Critically it should include the ability to monitor communications that span multiple communications and platforms.

Enforcement 4

Two brokers were found to have failed to reasonably supervise two registered representatives who engaged in a scheme to overcharge commissions to seven institutional customers, The firm prohibited representatives from making misleading statements in communications with the public and surveilled communications to detect potentially misleading statements. The communications surveillance team reviewed the communications flagged by its surveillance system but failed to examine the attached confirmations where representatives were misrepresenting commissions and misstating the share price.

As a result of a number of findings, in October 2022, the brokers were censured, fined a combined total of $1.1m, required to make restitution of $48,574.79 plus interest and required to certify that they had completed a review of their policies, procedures, and systems regarding the monitoring of electronic communications.

Relevant Regulatory Requirements

FINRA Rule 3110(a), like its predecessor rule NASO Rule 3010(a), requires that each member firm establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA Rules. The duty to supervise includes the responsibility to reasonably investigate red flags that suggest misconduct may be occurring.

Key Lessons:

Firms must have in place a suite of preventative and detective controls to seek to identify any instances of misconduct. In this instance representatives sought to conceal their misconduct by creating their own trade confirmations containing misleading information including understating commissions, which they then emailed to customers.

- Firms would be well advised to review their approach to electronic communications surveillance. In particular the approach should be reviewed to ensure that any communications flagged for review also have the attachments examined. It is insufficient for surveillance teams to review flagged communications without also reviewing any attachments, whether GIFs, videos, Sharepoint links or documents. Being able to fully review the content as well as the context requires a firm to be able capture and assess all emojis, reactions and edits that can change the meaning of communications.
- All compliance escalations should be routinely followed up. Whenever compliance testing identifies and escalates a concern, the issue should be followed up and the resolution documented in detail. Any findings can also be used to refine or update the associated suite of preventative and detective controls.

How Theta Lake can Help

Theta Lake's multi-award winning product suite provides patented compliance and security for modern communications utilizing over 100 frictionless partner integrations that include **RingCentral**, **Webex by Cisco**, **Microsoft Teams**, **Slack**, **Zoom**, **Movius** and more. Here's some of the ways Theta Lake can help you align with the better practices expected in the multiple FINRA enforcement actions:

- Theta Lake captures and compliantly archives communications including videos, voice, email (including attachments), chat, screen share and file transfer from mobile messaging platforms to SMS and WhatsApp to enable compliance with the relevant FINRA and other requirements. It also acts as an archive connector, enabling existing archives and data storage to be utilized without disruption.
- AI-enabled automated detection of potential misconduct. Identified risks are surfaced in an AI-assisted review workflow providing an efficient and effective review process for compliance teams. Theta Lake has more than 85 risk detections which are pre-trained and ready for customer use with customers able to provide feedback and training on the classifiers.
- There's complete flexibility to set retention periods to suit your needs. Theta Lake supports rapid identification, and consistent legal hold, of relevant communications, content and images across platforms to support investigations, regulatory review, audits or complaints.

- The ability to ensure that all aspects of messaging can be preserved, and a full audit trail provided to supervisors, regulators or prosecutors. For example, chat messages can be viewed in their native format over the entire history of the conversation with full context retained together with in-meeting communications and images, GIFs, emojis or reactions that change meaning and context.
- The ability to monitor communications, as well as enforce information barriers, across multiple platforms - supporting heightened supervision.
- Theta Lake's suite is SOC2, Type II audited and maps controls to ISO 27001 so confidential, privileged or sensitive data can be automatically redacted to meet data privacy and other legal obligations.
- Rich eDiscovery and search capabilities with capabilities across hundreds of search filters and metadata, as well as free-form text search across what is spoken, shown on screen, shared, or written.

IF YOU'D LIKE TO SEE HOW THETA LAKE CAN HELP, REQUEST A DEMO TODAY FROM OUR FRIENDLY TEAM.