The Companion Guide to FINRA/SEC Social Networking Compliance
Overview

Today financial firms generally fall in one of two camps when it comes to adopting social networking tools like Facebook, LinkedIn and Twitter. They have either blocked access because of the challenges associated with supervisory and data retention requirements or they’ve opened the doors to these sites and address compliance issues with highly manual processes.

Most are aware that FINRA has convened a social media task force to evaluate their compliance requirements for this new channel. On January 25, 2010, FINRA released Regulatory Notice 10-06 which provides additional guidance on the use of blogs and social networking sites.

With the release of Notice 10-06, FINRA makes it very clear that all communication via the Internet, including the social networks, is the same as in-person or written communication. As a result, this electronic communication can be considered correspondence, a public appearance, an advertisement or sales literature.

Remember, according to FINRA:

- Publicly available web sites (ex: Twitter) are considered advertisements
- An email or instant message sent to 25 or more prospective customers is considered sales literature
- An email or instant message is considered correspondence if it is sent to a single customer, an unlimited number of existing retail customers and/or less than 25 prospective retail customers (firm-wide) within a 30-day period
- Password-protected websites (ex: Facebook or LinkedIn) are considered sales literature
- Chat room discussions (ex: Facebook discussions, LinkedIn Q&A) are considered public appearances

Following is a summary of the key FINRA and SEC rules relevant to social media compliance. In addition, we’ve shared specific social network considerations and recommendations on how to participate with these networks in a compliant fashion. Firms should consider adopting a technology solution that is capable of both policy enforcement and moderation as well as archiving and supervision.

“"You have to find a way to supervise this activity””
FINRA, 2009

FINRA Rules Summary

1. Approval and Recordkeeping (Rule 2210)

“The content provisions of FINRA’s communications rules apply to interactive electronic communications that the firm or its personnel send through a social media site. While prior principal approval is not required under Rule 2210 for interactive electronic forums, firms must supervise these interactive electronic communications under NASD Rule 3010 in a manner reasonably designed to ensure that they do not violate the content requirements of FINRA’s communications rules.” *

Social Network Considerations

- While pre-approval for interactive content is not required under FINRA’s guidelines, it does require...
firms to adopt a reasonably designed policy and encourages firms to employ “risk-based principles” to determine the appropriate amount of review.

- Without automated policy-management tools, manual approval processes may create a compliance review bottleneck.
- Post-review is another option which requires the ability to do sampling and real-time lexicon-based searches.

**Compliance Recommendation**

Depending on the policy your firm defines, adopt a solution that automatically routes social media messages to a registered principal to accelerate the review process while providing a complete audit trail. And/or adopt a solution that provides automatic data retention for post-review and the ability to scan posts in real-time based on a lexicon of phrases or constructs.

### 2. Supervision (Rule 3010)

“Each member shall develop written procedures that are appropriate to its business, size, structure, and customers for the review of incoming and outgoing written (i.e., non-electronic) and electronic correspondence with the public relating to its investment banking or securities business.” *

**Social Network Considerations**

- Social networks offer multiple ways to communicate with customers from status updates, discussion boards, email and/or chat – all are considered electronic communications.
- Policies should account for the unique communication channels available on each social networking site.

**Compliance Recommendation**

Adopt a solution that enables firms to configure their supervisory rules of social network communication based on the FINRA guidelines as well as their own unique procedures and policies appropriate for their businesses.

### Regulatory Notice 10-06 Highlights

- Firms are required to archive and supervise communications to protect consumers from undue risk.
- Rules apply to firms and personnel using sites for business purposes (defined by the content of the message, not where site is accessed.)
- Social networking sites have both static and interactive content. For example, Twitter posts or Facebook status updates are considered interactive. Wall posts and profile information are static, requiring pre-approval or controlled access.
- Static content must be moderated (or pre-approved by a principal.)
- While interactive content does not require mandatory pre-approval, firms must supervise interactive content in a manner reasonably designed to ensure they do not violate communications rules.
- Customer complaints must be acknowledged and followed up within 15 days.
- FINRA is prepared to bring disciplinary action for violation of rules and securities laws.

### 3. Books and Records (Rule 3110)

“Advertisements and sales literature must be maintained as part of the firm’s records for three years from the date of last use. Correspondence must also be maintained in compliance with applicable FINRA rules and with SEC Rules 17a-3 and 17a-4. A registered representative’s (“RR”) email or instant messaging to the public relating to the firm’s business whether generated from the office, home or elsewhere, is subject to these provisions. RRs should know and
comply with their firm’s policies in this area.” *

Social Network Considerations

• Social networking activity (status updates, tweets, etc.) fall under the guidelines of an advertisement and/or sales literature.

• Sending an email using the social networks (Facebook Mail, LinkedIn Mail) or an instant message (Facebook Chat) can also be considered correspondence.

• Social networks can be updated at any time from any location. Firms must educate and provide the tools to capture and retain content that falls under the advertisement, sales literature or correspondence guidelines.

Compliance Recommendation
Adopt a solution that enables firms to capture and retain all social networking activity, with associated metadata, and archive this content in a structured fashion (enabling easy discovery). Additionally firms may choose to block access to certain features of these social networks.

4. Recommendations / Testimonials (Rule 206(4))

“It shall constitute a fraudulent, deceptive, or manipulative act, practice, or course of business within the meaning of section 206(4) of the Act for any investment adviser registered or required to be registered under section 203 of the Act, directly or indirectly, to publish, circulate, or distribute any advertisement: (1) Which refers, directly or indirectly, to any testimonial of any kind concerning the investment adviser or concerning any advice, analysis, report or other service rendered by such investment adviser.” *

Social Network Considerations

• Linkedin provides a simple mechanism to capture and display recommendations.

• Recommendations from non-clients may fall outside of the SEC guidelines, however given the amount of information that can be discovered through the associated profiles, it’s possible it could be perceived as a violation.

Compliance Recommendation
Adopt a solution that enables firms to selectively disable the ability to accept or request LinkedIn recommendations based on an individual’s role.

5. Third-Party Posts (Rule 2210 / Notice 10-06)

“As a general matter, FINRA does not treat posts by customers or other third parties as the firm’s communication with the public subject to Rule 2210. Thus, the prior principal approval, content and filing requirements of Rule 2210 do not apply to these posts.

Under certain circumstances, however, third-party posts may become attributable to the firm. Whether third-party content is attributable to a firm depends on whether the firm has (1) involved itself in the preparation of the content or (2) explicitly or implicitly endorsed or approved the content.” *

Social Network Considerations

• Republishing a comment from a third party, such as retweeting, will likely be considered an endorsement by the firm.

• “Favoriting” a post on Twitter or “Liking” a comment on Facebook can also be seen as an endorsement by the firm.

Compliance Recommendation
Adopt a solution that enables firms to disable the ability to Favorite or Like a Tweet or comment. Depending on an individual’s risk profile, you may choose to adopt a solution that provides pre- and post-moderation for any retweeted messages.

For additional information from FINRA on the compliance concerns surrounding social networks, we would encourage you to download Regulatory Notice 10-06 in its entirety: http://bit.ly/Notice1006 or visit our online resource center at http://www.smarsh.com.

* FINRA’s Guide to the Internet for Registered Representatives, SEC’s Rules Under the Investment Advisers Act of 1940, FINRA Regulatory Notice 10-06
SEC Rules Summary

1. Retention (Rule 17a-3 and 17a-4)
“In combination, Rules 17a-3 and 17a-4 require broker-dealers to create, and preserve in an easily accessible manner, a comprehensive record of each securities transaction they effect and of their securities business in general.” **

Social Network Considerations
• Social network content is electronic communication and should be captured, indexed and preserved according to 17a-3 and 17a-4.

Compliance Recommendation
Adopt a solution that archives and retains social networking content from Facebook, LinkedIn and Twitter.

2. Indelible Preservation (Rule 17a-4)
“Requires broker-dealers to...preserve the records exclusively in a non-rewritable, non-erasable format.” **

Social Network Considerations
• Social networking content should be stored to Write-Once-Read-Many (WORM) media.
• Social networking messages, status updates, and content should be preserved in their native, unaltered formats. Taking intermittent point-in-time snapshots or modifying these messages to fit an email format is at fundamental odds with the archiving requirements of 17a-4.

Compliance Recommendation
Adopt a solution that stores all social networking activity to WORM optical media and captures data in real-time.

3. Accessibility (Rule 17a-4)
“Have the capacity to readily download indexes and records preserved on electronic media storage media to any medium... as required by the SEC or the self-regulatory organizations of which the member, broker, or dealer is a member [such as FINRA].” **

Social Network Considerations
• Archived social networking content should be readily accessible.
• Content should be easily searchable by specific fields and efficiently exportable.

Compliance Recommendation
Adopt a solution that keeps data readily accessible via a search and retrieval interface that can scale with your message archive growth, assuring your ability to produce content upon request from an examiner or auditor.

4. Redundancy (Rule 17a-4)
“Store separately from the original, a duplicate copy of the record.” **

Social Network Considerations
• Data protection and preservation is paramount. Records should be stored in secure, independent locations, with at least one of the copies stored offsite.

Compliance Recommendation
Your firm or archiving provider should preserve and store your data in a fully redundant, secure, and highly available environment.

5. Audit Trail (Rule 17a-4)
“The member, broker, or dealer, must have in place an audit system providing accountability...and inputting of any changes made to every original and duplicate record maintained and preserved thereby.” At all times, such audit system must be “available for examination by the staffs of the SEC and self-regulated organizations [such as FINRA].” **

Social Network Considerations
• Maintaining a full audit trail of all archival and supervision actions of social networking activity is necessary.

Compliance Recommendation
Adopt a solution that has a full audit trail for both pre-review (moderation) as well as post-review (surveillance...
and supervision), and tracks metadata associated with the archival and review process (notes, tags, review assignment, etc.)

6. Third-Party Rule (Rule 17a-4)
“For every member, broker, or dealer exclusively using electronic storage media for some or all of its record preservation under this section, at least one third party... who has access to and the ability to download information... shall file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records.” **

Social Network Considerations
• Attestation letters, citing the ability to produce a client’s data if necessary, should be provided to FINRA and the SEC from an independent third party with access to electronic records.
• Upon SEC (or FINRA) request, it is important to have export capabilities so that social networking communication can be furnished alongside other electronic communication (such as email, instant messaging and Bloomberg messages.)

Compliance Recommendation
Identify a third-party provider with regulatory audit experience and that is capable of making (and fulfilling) attestations on behalf of clients.

7. Data Protection (Regulation S-P)
The SEC adopted Regulation S-P in accordance with Section 504 of the Gramm-Leach Bliley Act (GLBA) requiring brokers, dealers, investment firms and investment advisors to implement safeguards and define standards to protect non-public consumer information.

Social Network Considerations
• Establish appropriate standards to protect customer information including access control and supervision.

Compliance Recommendation
Adopt a solution that restricts access to high-risk features of social networking sites, helping protect against data breaches. Firms should also safeguard and supervise all archived electronic communication, including social networking activity, to mitigate organizational risk and comply with Regulation S-P.


Requirements for Social Networking Compliance
By implementing a social networking compliance solution, you can protect your firm from compliance fines and expensive legal fees. The solution you choose should provide the following capabilities:

Automatic discovery of social network accounts across any regulated representative
Regardless of the number of social networking accounts that a user has, the system will detect them and enforce the compliance rules defined by your firm.

Automatic capture of social networking data impacted by FINRA/SEC policies
Depending on the type of data flowing across the social networks, your compliance solution needs to be flexible enough to automatically capture the data and classify it accordingly. For example, a profile update should be flagged and treated differently than a status update.

Archived content should be written to WORM media
All archived data must be preserved in its original form on tamper-proof media.

Ability to export data efficiently during internal investigations, regulatory audits or discovery events
Your export process should allow you to pick and choose which data and data types to be exported. Combining multiple searches and message types will create a more effective and efficient review process.

Independent Third Party Attestation
Choose an established third-party download provider with experience helping clients pass regulatory audits.
Ability to search and export social network data
As you aggregate massive amounts of social network content, your ability to produce it will be critical. Your compliance solution should scale and allow you to conduct advanced searches.

Automated routing of social networking messages that require pre-approval
For situations where prior approval is required, your compliance solution needs to capture the content before it posts, route it to a defined moderator and, once moderated, capture the associated details.

Automatic posting of moderated social networking messages once approved
Once a message has been moderated and approved, your compliance solution should enable one-click publishing of the content on behalf of the user.

Ability to capture metadata associated with a social network post or activity
Understanding the surrounding context of a post is as important as the post itself. At a minimum, the system must capture additional detail such as the enterprise user credentials, URL of the page and the reference post when making a comment.

Ability to restrict access to social networking features on a user-by-user basis
The ability to block accepting recommendations on sites, like LinkedIn, helps ensure end-users don’t inadvertently violate compliance policies. The solution you choose should provide the flexibility to block features most vulnerable to compliance risk.

Integration of access control and moderation capabilities with archiving and supervision features
For many organizations, a single archival solution for multiple content or message types is important for supervisory efficiency and mitigation of risk.

Ability to scan for keywords and phrases
Content posted to social networks gets created quickly and spreads even faster. Manual review of all content can quickly become impractical if not impossible. Automatically scanning and capturing content that doesn’t pass your filters is an invaluable part of any social network compliance solution.

Ability to assign messages to reviewers
For many organizations, email and electronic message review is handled by a team. Create a more efficient review process including load-balanced, “assign to reviewer” tools to ensure supervision is taking place.

Built in tools to help create a reasonably designed set of policies and procedures
Choose a solution that has advanced pre-and post-review capabilities, including moderation and pre-approval of interactive posts, and risk-based (identifying high-risk users) sampling and lexicon-based post review.

Built-in reporting capabilities on usage, captured content and moderation activity
What is measured gets proved and improved. Your social networking investment is no different. Your compliance solution should give you real-time insights to individual and group usage, rule violations audit history and moderation queues.

About Smarsh
Smarsh® provides hosted solutions for archiving electronic communications, including email, instant messaging and social media platforms. Founded in 2001, Smarsh helps over 10,000 organizations manage and enforce flexible, secure and cost-effective compliance and records retention strategies and mitigate risk. The Smarsh social media compliance solution integrates ground-breaking middleware technology from Socialware, a leader in helping companies manage, embrace and leverage public social networks.

Call Today
1-866-SMARSH-1
www.smarsh.com | sales@smarsh.com

Smarsh, Inc. assumes no liability for the accuracy or completeness of this information. Please consult with an attorney for specific information on specific rules and regulations and how they apply to your business.