

FINRA COMPLIANCE GUIDE

Social Networks, Web 2.0, and Unified Communications



Table of Contents

Executive Summary	3
Social Networking Does Not Occur in Isolation.	4
Risks Beyond Being Out of Compliance.	5
Data Leakage	6
Inbound Threats	6
Compliance	6
User Behavior	7
Key Rules	8
NASD Rule 2210 (Communications with the Public)	8
NASD Rule 3010 (Supervision)	9
NASD Rule 3110 (Books and Records)	9
FINRA - Key Notices	10
Notice 07-59 (Conflicts of Interest)	10
Notice 10-06 (Social Media Websites)	10
How Actiance Meets FINRA Compliance Requirements.	11
Socialite	11
Ten Steps to Social Networking Compliance.	12
About Actiance, Inc.	13

This white paper is for informational purposes only. Actiance makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Actiance, Inc. © 2001 - 2011 Actiance, Inc. All rights reserved. Actiance and the Actiance logo are registered trademarks of Actiance, Inc. Actiance Vantage, Unified Security Gateway, Socialite, and Insight are trademarks of Actiance, Inc. All other trademarks are the property of their respective owners.

Worldwide Headquarters
1301 Shoreway, Suite 275
Belmont, CA 94002 USA
(650) 631-6300 phone
info@actiance.com

EMEA Headquarters
400 Thames Valley Park
Reading, Berkshire, RG6 1PT UK
+44 (0) 118 963 7469 phone
emea@actiance.com

actiance™

Executive Summary

In January 2010, FINRA issued Regulatory Notice 10-06, its latest guidance in a series on electronic communications specifically related to social media websites. There are currently 519 million Facebook users, 65 million LinkedIn members, and 190 million Tweeters. The growth in social networking sites is huge, not least because of the variety of ways it offers for people to communicate, but also the speed, allowing for deals to be closed quickly and information to be relayed without delay.

However, when considering the results of a recent survey conducted by Actiance which showed that Web-based chat was used in 95% of organizations and file sharing tools were found to be present in 74% of locations, it is clear that Regulatory Notice 10-06 should not just be taken in isolation when meeting FINRA compliance. Enterprises must consider a broader swath that includes Unified Communications (UC), instant messaging (IM), and Web 2.0 applications, alongside social media to remain in compliance.

Many Internet-based and Web 2.0 applications are specifically designed to evade legacy security solutions like URL filters and firewalls; others pose challenges in monitoring content and archiving. However, the benefits from using them are proving so great that it is easy for Registered Representatives (RRs) to forget their compliance obligations.

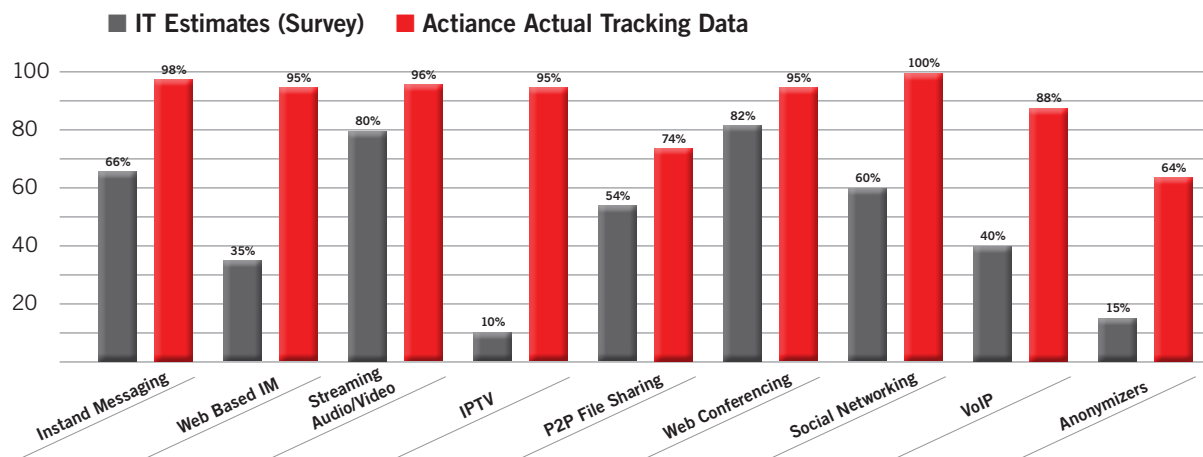
This whitepaper sets out some of the key rules, guidelines and associated risks for FINRA member firms and suggests ways that organizations can use technology to protect themselves and their RRs. In addition, it looks at some of the other issues that enterprises may encounter when enabling the new Internet.

Social Networking Does Not Occur in Isolation

It took the humble telephone eighty-nine years to reach the 150 million users that Facebook achieved in just five. The phenomenal growth of Web 2.0 and social networks has undoubtedly driven the growth in enterprise UC tools such as Microsoft OCS, IBM Lotus Sametime, and Thomson Reuters Messenger. However, just because an organization has standardized on an enterprise tool does not mean it should overlook the use of Facebook, LinkedIn, and Twitter on its network.

In Actiance's Fifth Annual Internet Usage Survey, which compares IT estimates against live, anonymized data from 150 Actiance-deployed appliances, over 99% of end users had adopted social media and Web 2.0 applications to support business processes. Conversely, 38% of IT professionals believed there was no social networking present on their network.

This same survey showed 53% of end users downloading and using tools such as Facebook and LinkedIn because they "were better than those provided by my employer".



Source: The Collaborative Internet. Usage Trends, End User Attitudes and IT Impact, Actiance, 2010

Enterprise communication tools still have their place within an organization, but users will always look to communicate in the easiest method. If their customer is conversing over Yahoo or Skype, users will try to access the relevant Web 2.0 application. Similarly, social networking sites such as LinkedIn and Facebook are now standard tools for savvy marketers and sales people.

The Citi Cards division of Citibank is just one of a number of banks that are already using social networking to build a community around its brand. It launched a campaign that centers on the power of harnessing a user's network on Facebook, by offering to donate \$50 to charity for every approved credit card application from a user's "friend". Bank of America is using Twitter, not to sell, but as an extension of their customer service support, answering queries quickly, taking them to a more secure communications channel if sensitive information is required.

All these real-time communications applications, whether it's enterprise 2.0, Web 2.0, or social networking are just extensions of normal everyday conversations that used to take place over the phone or email. However, it is not without risk, many applications and sites use port hopping, protocol tunneling, and encryption techniques to enable them to work seamlessly, and frequently undetected, on the network, providing outlets for malware and data leakage.

Risks Beyond Being Out of Compliance





The risks that Web 2.0, social media, and enterprise collaboration tools pose are very similar to those of other electronic communications like email: malware, data leakage, potential libelous comments, non-compliance with government and industry regulations, and hefty litigation and eDiscovery costs. Just like email, the principles for applying policies and securing these new types of communications remain the same.

Most businesses have implemented numerous technologies to counteract the risk associated with email, from content control filters that prevent inappropriate emails from escaping the corporate network to anti-malware software that protects both employees and the people they interact with everyday. All backed-up by a fully audited archive.

However, unlike email, because Web 2.0, social media, and enterprise communications and collaboration tools cover such a wide range of modalities – from instant messaging to Twitter and from IPTV to playing games on Facebook – consideration should be given to types of applications, their individual capabilities, and the associated risks.

The problem for regulated financial institutions is that inappropriate use of such widely available communications and collaboration tools can mean non-compliance with government and industry regulations, resulting in hefty fines, potential loss of business, and fraud. In 2010, FINRA fined Piper Jaffray \$700,000 for failure to retain approximately 4.3 million emails from November 2002 through December 2008. And in November 2009, FINRA levied a huge \$1.2 million fine against MetLife for failing to establish an adequate supervisory system for the review of brokers' email correspondence with the public.

More recently, Societe Generale lost nearly €4.9 billion in fraudulent trades by a rogue employee that used instant messaging to manage the transactions. Also, news that Zicam, a nasal spray form of cold remedy produced by Matrixx Initiatives, had potentially been found to damage some peoples' sense of smell was first revealed in tweets on June 15, 2009. Matrixx' stock price that day went from \$19.24 to \$5.78. It's not been higher than \$6.55 since.

Data Leakage	Incoming Threats	Compliance & eDiscovery	User Behavior
			
Personal Information Intellectual Property Credit Card, SSN Client Records	Malware, Spyware Viruses, Trojans Inappropriate Content	SEC, FINRA HIPAA FISMA SOX, PCI FRCP- eDiscovery Ferc, NERC	Employee Productivity Bandwidth Explosion Every employee is the face of business

Web 2.0, social media, and real-time communications risks

Data Leakage

Data leakage through social media and Web 2.0 applications is now a significant threat. In Actiance's annual survey, 69% of IT respondents reported incidents of malware and/or information leaks due to the use of Internet applications. Viruses were most common at 55 percent, followed by spyware infiltrations at 45 percent – but in new statistics gathered for the first time this year, 14% have seen data leakage through social networks.

The problem with Web 2.0 applications such as IM, Skype, and the chat functions within Facebook is that they can easily traverse the network without being seen, potentially allowing credit card details, confidential trading information, client records, and the like to leave the organization unauthorized. If these applications cannot be seen then they cannot be managed or secured, resulting in a significant risk of falling out of compliance.

There is also the potential for accidental leakage, too, and not just from sending an IM to the wrong person. For example, each of the 60,000 applets on Facebook requires users to download a small executable file that accesses a user's profile, potentially retrieving information and even allowing malware in.

Inbound Threats

Just like email, malware writers relish the opportunity to apply the latest social engineering techniques to persuade users to install their spyware and viruses. One of the main reasons for the hackers and malware writers' success rate is that many users place too much trust in their network. Even though they may not know who their "friends" are in the real world, a feeling of trust builds up over a period of time. This makes users far more likely to click on a link from a friend on Facebook, LinkedIn, or Twitter than in an email, where most people today are a bit more circumspect, particularly if it's unexpected.

Inappropriate content, whether it is a comment that could be construed as advertising or a recommendation, a libelous statement about a competitor, or just a really humiliating picture on Facebook, if the person is a recognizable employee, it could compromise the whole organization. Consideration must also be given to the features within social media sites that may also inadvertently run afoul of applicable regulations.

Compliance

Virtually all company data is subject to discovery should legal action be taken, including communication traffic over Web 2.0, social media, and unified communications. At the end of the day, these are all simply forms of "electronic communications." In order to comply with most industry and government regulations, including FINRA, organizations need to demonstrate sufficient supervisory review, approval, and retention procedures and capabilities are in place. However, in practice, not many firms are able to log content posted to Facebook, let alone try to control the content of the actual message.

The process of archiving, storing, and making these conversations and posts easily retrievable for regulatory compliance and legal discovery is made exponentially more complex by the multi-dimensional nature of these conversations. For example, a chat conversation can include numerous participants joining at different times, creating a requirement to understand the context surrounding each participant's understanding of these conversations. For instance, who entered and left the conversation at what point during the discussion? Within financial industries, this is normally taken a step further and the use of ethical walls between business functions is a required element of compliance.

There are additional regulations outside of FINRA guidelines that relate to Web 2.0, social media, and enterprise communications:

Regulation or Rule	Impact
Gramm-Leach-Bliley Act (GLBA)	Information protection, monitor for sensitive content and ensure not sent over public channels (e.g., Twitter)
Investment Advisers Act of 1940	Investment advisers are prohibited from publishing, circulating, or distributing any advertisement 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.
SEC 17a-3 and 17a-4	Specifies the types of electronic records that must be preserved. Also specifies the manner and length of time that the records maintained by broker-dealers must be preserved.
PCI	Ensuring cardholder data is not sent over unsecured channels and proving it has not occurred.
Red Flag Rules	Prevent identity theft. Protect IM and Web 2.0 from malware and phishing where users are more likely to let down their guard.
Federal Rules of Civil Procedure (FRCP)	Email and IM are ESI (Electronically Stored Information). Posts to social media sites must be preserved if reasonably determined to be discoverable.
Sarbanes-Oxley (SOX)	Businesses must preserve information relevant to the company reporting. This means all IM and social media “conversations” are relevant.
Canadian Securities Administrators National Instrument 31-303 (CSA NI)	Retain records for two years in a manner that allows “rapid recovery to a regulator”. Can extend to IM and social media.
Investment Dealers Association of Canada (IDA29.7)	Requires the retention of records with respect to business activities, regardless of its medium of creation.
MiFID and FSA: Markets in Financial Instruments Directive (EU)	Specifically requires the retention of electronic communications conversations when trades are referenced.
Model Requirements for the management of Electronic Records (MoReq)	European requirements that define the functional requirements for the manner in which electronic records are managed in an Electronic Records Management System.

User Behavior

Web 2.0 and social media offer huge productivity benefits, but that doesn’t mean employees should be given a free rein. Consideration should still be given to whether an employee really needs access to specific applications or be able to transfer certain files types.

Unlike many other industries, Registered Representatives are duty bound to follow the rules and regulations surrounding electronic communications even during their “own time”, if they are identifiable as a representative of the organization. Members of the marketing team might understand what is appropriate to post to Facebook or indeed what process to follow to post, but “John” in the mailroom might not. His posts or photographs from weekend parties might not be suitable content.

Key Rules

NASD Rule 2210 (Communications with the Public)

Under NASD Rule 2210(b), FINRA expressly points out that “instant messaging to 25 or more existing customers over a 30 day period requires prior approval by a registered principal”. However, in Regulatory Notice 10-06, FINRA does concede that in interactive electronic forums, such as chat rooms, prior approval of extemporaneous remarks is not required but cautions that these types of communications are subject to other supervisory requirements and to the content requirements of FINRA’s communications rule.

Compliance considerations

- Regulatory Notice 10-06 does pave the way for RRs to participate in real-time communications, but care still needs to be given to the content of the message.
- Under NASD 2210, communications with the public must be based on the principles of fair dealing; misleading statements, exaggerated claims, and predictions of investments are strictly forbidden.
- Retweeting or republishing a comment from a third party is likely to be considered as an endorsement, as is “liking” a comment on Facebook or LinkedIn, thus, caution is urged.
- Rule IM-2210-1 states that every member is responsible for determining whether their statements are compliant.

Compliance recommendations

Given that human error or judgment is frequently found to be a contributing factor in most adverse situations, organizations began implementing content filtering systems for their email platforms a long time ago. Companies need to implement a solution that provides content filtering for messages posted to a wide range of real-time communication tools, social networking sites, and webmail (e.g., Gmail) to ensure that all messages are appropriate.

Consideration should be given to disabling the ability to “like” or “retweet” or “favorite” for certain representatives within the organization.

Notification to users about why a particular message was blocked can help to train individuals further and deter repeat offenders. Reinforcing procedures is particularly critical since FINRA explicitly points out in its Guide to the Internet that even where a communication is made by a representative of a FINRA member firm outside of the office (e.g., from home), if it concerns investments, then it falls under FINRA regulations.

NASD Rule 3010 (Supervision)

“Members must establish, maintain and enforce written procedures for communications”; the inclusion of electronic communications was confirmed in Notice 99-03. Furthermore, 10-06 reminds members that under NASD Rule 3010 members must supervise social media communications “in a manner reasonably designed to ensure that they do not violate the content requirements of FINRA’s communications rules”.

Compliance considerations

- It is not possible to supervise communications if the organization does not have visibility of all electronic communication tools in use on its network.
- Even if an enterprise has standardized on its use of electronic communications tools, it does not prevent users from downloading other applications. Most real-time communication and Web 2.0 applications have been specifically designed to avoid detection by traditional security measures.

Compliance recommendations

In order to be able to enforce communication policies, enterprises need to implement technology that is able to provide visibility into all real-time communication tools and Web 2.0 applications on the network and the ability to block or control their usage.

NASD Rule 3110 (Books and Records)

“Each member shall make and preserve books, accounts, records, memoranda, and correspondence in conformity with all applicable laws, rules, regulations and statements of policy promulgated thereunder and with the Rules of this Association and as prescribed by SEC Rule 17a-3. The record keeping format, medium, and retention period shall comply with Rule 17a-4 under the Securities Exchange Act of 1934.” Furthermore, 10-06 reminds members that firms which communicate through social media sites must still adhere to these rules.

Compliance considerations

- Social networking sites, such as Facebook, offer no native archiving functionality, making it difficult to comply with Regulatory Notice 07-59 that spells out the requirements for review “by a supervisor of employees’ incoming, outgoing and internal electronic communications.”
- Native archiving functionality offered by unified communications and other real-time communications tools is rarely able to provide a granular breakdown of conversations by persons (including buddynames), key phrases, and timeframes, which are essential for compliance and eDiscovery requirements.
- This is further complicated by the slew of modalities used in conversations – from IM to BlackBerrys.

Compliance recommendations

Enterprises should deploy a central archiving system that enables easy review of posted messages and detailed analysis of electronic conversations, including file downloads both internally and externally, complete with an audit trail of the auditor reviewing the information. In addition, the information should include who joined a conversation, when and when they left, any disclaimers shown (at the beginning of an IM conversation, for instance), and call detail records (CDRs) for voice calls, group meeting sessions, etc.

FINRA – Key Notices

Regulatory Notice 07-59 (Conflicts of Interest)

In the ever-expanding role of electronic communications in Regulatory Notice 07-59, Supervision of Electronic Communications, FINRA suggests that members consider taking steps “to reduce, manage or eliminate potential conflicts of interest, to prevent electronic communications between certain individuals/groups or monitoring communications as required by FINRA rules.”

Compliance considerations

- In certain situations, there may be a requirement to restrict electronic conversations between internal personnel such as non-research and research departments. In addition, there may be a requirement to restrict electronic communications between specific persons from different organizations, while still allowing broad communication with others.
- Though it is easy for a registered representative to recognize in a one-to-one instant message conversation whether or not they should be talking to the individual, with the popularity of features such as Microsoft’s Group Chat, it is now a considerable risk.
- Multi-party communications (e.g., chatrooms, Live Meetings, etc.) make it easy for individuals to accidentally infringe upon FINRA’s various conflict of interest regulations.

Compliance recommendations

Implement ethical walls at both a group and domain level to ensure that conflicting personnel do not accidentally “meet” electronically and to maintain a full audit trail that clearly displays when an individual joined a meeting and subsequently left. In addition, the use of disclaimers when a member joins a meeting can help to reinforce the message.

Regulatory Notice 10-06 (Social Media Websites)

The release of Regulatory Notice 10-06 from FINRA makes it very clear that all electronic communications shared via the Internet should be treated in just the same way as if it were shared in person or in non-electronic written communications.

Compliance considerations

- Social media is a dynamic medium that relies on real-time (or near real-time) interaction between participants to be a useful resource for information and communication. Allowing unfiltered access raises the possibility of an employee accidentally or deliberately saying something inappropriate.
- Moderating every post manually will increase the overhead of using social media and may also add an element of delay in the “conversation” that offsets the benefit of using the medium.

Compliance recommendations

Educate users to understand what is considered appropriate content. Implement filters that can control the content posted to sites such as Facebook, LinkedIn, and Twitter and enable the automation of the moderation process where applicable.

How Actiance Meets FINRA Compliance Requirements

Socialite

Socialite is Actiance's security, management, and compliance solution for Social Networks, providing granular control of Facebook, LinkedIn, and Twitter. Socialite not only controls access to 150 different features across social networks, but can also moderate, manage, and archive any social media traffic routed through the solution, which can either be on-premise or hosted.

Socialite includes a number of key features for securely enabling the use of social networks, including:

- **Data leak prevention:** preventing sensitive data from leaving the company, either maliciously or inadvertently
- **Identity management:** establishing a single corporate identity and tracking users across multiple social media platforms (e.g., @JohnJones on Twitter is the same as JohnHJones on LinkedIn)
- **Activity control:** managing access to features, such as who can read, like, comment upon, or access specific features
- **Moderator control:** pre-approving content for Facebook, LinkedIn, and Twitter, where content is required to be reviewed by a corporate communications officer or other third party
- **Granular application control:** enabling access to Facebook but not to Facebook Chat or downloading/installing any of the applications in the gaming category
- **Conversation and content logging:** capturing all posts, messages, and commentary in context, including export to an archiving platform of your choice for eDiscovery purposes

Ten Steps to Social Networking Compliance

1. Gain visibility into all communications tools

The first step in any security review is to carry out an audit. Even if the use of real-time communications and Web 2.0 applications has been banned within the enterprise, the likelihood is users will have found a way to circumvent any measures put in place.

2. Develop policies under FINRA guidelines

An acceptable use policy (AUP) will let users know exactly what they can and can't do with respect to UC, IM, and Web 2.0 applications. Don't forget to include that the organization has the right to monitor all traffic and to remind registered representatives that they are bound by FINRA regulations, even if they are not using the company network.

3. Implement monitoring technology

The only way to see who is using what, how often, and when is to implement monitoring technology. Even if a business chooses to ban specific real-time applications or social networking sites, without monitoring in place, they can never be certain that users are actually complying.

4. Ensure Granular Access

Not all employees need access to every aspect of real-time communication tools or Web 2.0 applications. In the same way organizations block certain file types (e.g., only the marketing department can receive GIFs and JPEGs), consider limiting the various types of real-time communications by job function.

5. Apply policy management and control

Apply centralized policy management and control with a single solution for all elements of Web browsing, UC, and IM in use in the enterprise. Use Active Directory integration to set and enforce global-, group-, and individual-level real-time communications policies.

6. Enable Content Filtering

Ensure content posted and messages sent, whether via Web 2.0 applications such as Facebook or real-time communications tools such as Skype, can be monitored and blocked where necessary.

7. Implement Ethical Walls

Prevent registered representatives from inadvertently meeting forbidden personnel within official chatrooms.

8. Use Disclaimer Messages

Customizable disclaimers can not only make third parties aware of limitations, they can also be used to remind users of their obligations before entering into discussions.

9. Archive

Whether you need to retrieve messages for legal litigation, to substantiate a compliance issue, or just to confirm a contractual modification, all business messages need to be stored securely.

10. Don't forget about malware and data leakage

Protect the network by detecting and blocking incoming infections and existing endpoint infections when the spyware starts trying to 'phone home.'

About Actiance

Actiance enables the safe and productive use of unified communications, collaboration, and Web 2.0, including blogs and social networking sites. Formerly FaceTime Communications, Actiance's award-winning platforms are used by 9 of the top 10 US banks and more than 1,600 organizations globally for the security, management, and compliance of unified communications, Web 2.0, and social media channels. Actiance supports all leading social networks, unified communications providers, and IM platforms, including Facebook, LinkedIn, Twitter, AOL, Google, Yahoo!, Skype, Microsoft, IBM, and Cisco.

More Information

For more information about Actiance and its award-winning platform, please visit <http://www.actiance.com>.

Worldwide Headquarters

1301 Shoreway, Suite 275
Belmont, CA 94002 USA
(650) 631-6300 phone
info@actiance.com

EMEA Headquarters

400 Thames Valley Park
Reading, Berkshire, RG6 1PT UK
+44 (0) 118 963 7469 phone
emea@actiance.com