FaceTime®

WHITE PAPER

FINRA: Compliance Guide Social Networks, Web 2.0 and Unified Communications

FaceTime Communications, Inc.

Contents

WP101-0710 FINRA

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 web sites. There are currently 519 million Facebook users, 65 million members on LinkedIn and 190 million Twitterers. 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 FaceTime Communications 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 wider remit that includes Unified Communications, 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 organisations 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.

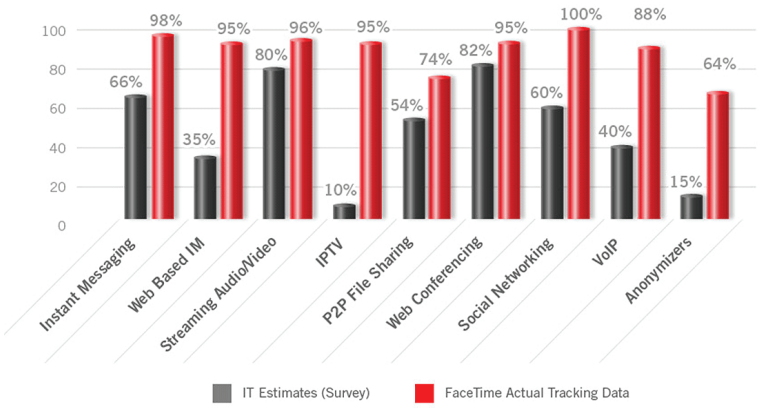
Social Networking Does Not Occur in Isolation

It took the humble telephone eighty-nine years to reach the hundred and fifty 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 Unified Communciation (UC) tools such as Microsoft OCS, IBM Lotus Sametime and Reuters Messaging. However, just because an organization has standardized on an Enterprise tool it is not a prerequisite for the elimination of Facebook, Twitter and LinkedIn from the network.

In FaceTime's Fifth Annual Internet Usage Survey, which compares IT Estimates against live (anonymized) data from 150 FaceTime 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".

Employee Use of Internet Applications: *Comparison of Estimated VS. Actual Usage*



Source: The Collaborative Internet. Usage Trends, End User Attitudes and IT Impact, March 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 communication applications whether it's Enterprise 2.0, Web 2.0 or Social Networking are just an extension 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 an entry point for malware and exit for data leakage.

Risks Beyond Being Out of Compliance

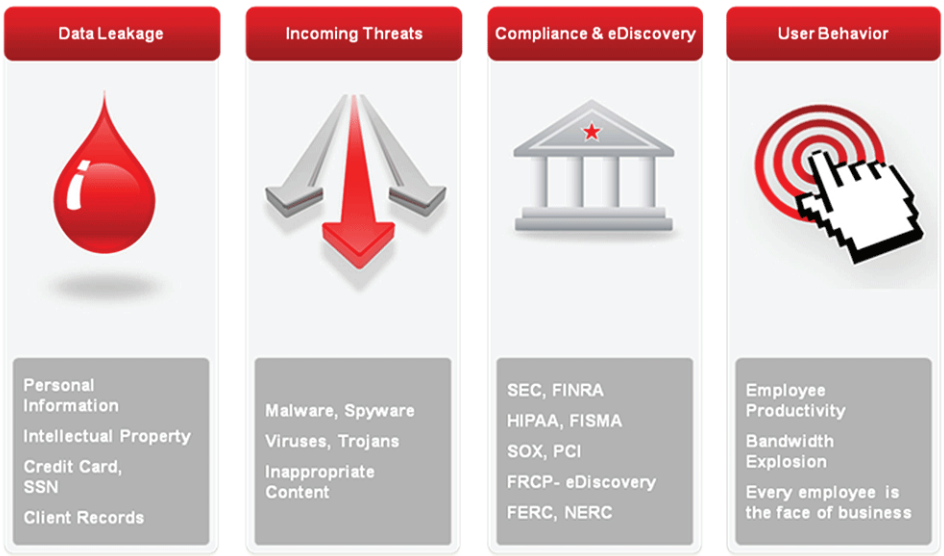
The risks that Web 2.0, Social Media and enterprise collaboration tools pose are very similar to those of other electronic communications such as email: malware, data leakage, potential libellous comments, non-compliance with government and industry regulations, and expensive litigation or eDiscovery 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 unsuitable 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 Communication tools cover such a wide range of modalities, from instant messaging to Twittering 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 communication 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.

More recently, Societe Generale lost nearly €4.9 billion in fraudulent trades by a rogue employee that used instant messaging to manage the transactions. 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 Twitter discussions 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.



Web 2.0, Social Media and Real-time communication risks

Data Leakage

Data leakage through social media and Web 2.0 applications is now a significant threat. In the FaceTime Fifth Annual Collaborative Internet 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 like 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 violating 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 that gives access to a user's profile, potentially retrieving information and even allowing malware in.

Inbound Threats

Just like email, malware writers like to make full use of 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 friend on Twitter, Facebook or LinkedIn than in an email, where most people today are a little more circumspect, particularly if it's unexpected.

Inappropriate content, whether it is a comment that could be construed as advertising or 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 organisation. Consideration must also be given to the features within social media sites that can also inadvertently break regulations.

Whilst still a theoretical problem, LinkedIn's Recommendations feature that allows testimonials to be posted to a user's LinkedIn page likely violates Rule 206(4)-1(a)(1) of the Investment Advisors Act of 1940. This could be a serious problem for any registered representative that currently has recommendations on their LinkedIn page.

Compliance

Virtually all company data is subject to discovery should legal action be taken, including communication traffic over Web 2.0, Social Media and UC. At the end of the day, this is all simply electronic communications. In order to comply with most industry and government regulations including FINRA, organisations need to demonstrate information control, retention and review. However, in practice not many firms are able 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 because of the multidimensional 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 participants understanding of these conversations – 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 specific regulations outside of FINRA guidelines that relate to Web 2.0, social media and enterprise communications:

Regulation	Impact
Gramm-Leach-Bliley (GLBA)	Info protection, monitor for sensitive content and ensure not sent over public channels (ex. Twitter)
SEC and FINRA	Obliged to store records and make accessible. Public correspondence requires approval, review and retention. Extended to social media.
PCI	Ensuring cardholder data is not sent over unsecured channels and proving it has not happened.
Red Flag Rules	Prevent identity theft. Protect IM and Web 2.0 from malware and phishing where users more likely to put down their guard.
FRCP (e-Discovery)	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 includes all IM and social media "conversations" is 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)	Demands the retention of records with relation 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 to say that 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. Although it points out 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 free 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 replublishing a comment from a third party is likely to be considered as an endorsement, as is "liking" a comment on Facebook or LinkedIn and caution should be urged in this instance.
- 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 implemented content filtering for their email systems 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 (eg Gmail) to ensure 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 highlight repeat offenders. Re-enforcing procedures is particularly critical since FINRA explicitly points out in its Guide to the Internet that even where communication is made from a representative of a FINRA member firm outside of the office, at home for instance, if it concerns investments then it comes 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 infrastructure.

Compliance recommendations

In order to be able to enforce communication policies, enterprises need to implement technology that is able to provide visibility of 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 that 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 sets out the requirements for review "by a supervisor of employees' incoming, outgoing and internal electronic communications".
- Native archiving functionality offered by UC and other real-time communication tools is rarely able to provide a granular breakdown of conversations by persons (including buddynames), key phrases and timeframes, essential for compliance and eDiscovery requirements.
- This is further complicated when a variety of modalities is used in a conversation from IM to Blackberry.

Compliance recommendations

Enterprises should deploy a central archiving system that enables easy review of messages posted 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 CDR information on voice calls, group meeting sessions etc.

Investment Advisors Act 1940 (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 which refers, directly, or indirectly, to any testimonial of any kind concerning the investment advisor or concerning any advice, analysis, report or other service rendered by such investment adviser."

Compliance considerations

- Consider ensuring that the ability to "like", "favorite", or recommend across social networks is disabled for registered representatives

FINRA - Key Notices

Notice 07-59 – Conflicts of Interest

In the ever expanding role of electronic communications in 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 communication between specific people from different organizations, whilst still allowing broad communication with others.
- Though it is easy for an RR to recognize in a one to one instant message conversation whether or not they should be talking to the individual, with the uptake of service such as Microsoft's Group Chat it is now a considerable risk.
- Multi-party communications such as chatrooms, live meetings etc make it easy for individuals to accidentally infringe of 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 maintain a full audit trail that clearly displays when an individual joined a meeting and subsequently left. In addition, the use of disclaimers when using UC platforms such as Microsoft OCS and IBM Lotus Sametime as member join a meeting can help to reinforce the message.

Notice 10-06 – Social Media Web Sites

The release of 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 non-electronic written communications.

Compliance considerations

- Social media is a dynamic medium that relies on quick 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 negates the befit 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 Twitter, LinkedIn and Facebook and enable the automation of the moderation process where applicable.

How FaceTime Meets FINRA Compliance Requirements

FaceTime Communications

FaceTime Communications enables the safe and productive use of Unified Communications and Web 2.0 – including social networks, blogs and instant messaging. Ranked number one by IDC for five consecutive years, FaceTime's award-winning solutions are used by more than 1,500 customers for the security, management and compliance of real-time communications. FaceTime supports or has strategic partnerships with all leading public IM network and Unified Communications providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM and Cisco.

Socialite

Socialite is FaceTime's Security Management and Compliance for Social Networks solution providing granular control of Facebook, LinkedIn and Twitter. Available as a hosted software-as-a-service deployment, on premise (as module of FaceTime's Unified Security Gateway) or as a hybrid combination of both.

Socialite ("social: IT-enabled") is a discrete feature set of FaceTime's security, management and compliance solutions for unified communications, and Web 2.0 to extend control over social media features and conversations to remote users (and smaller enterprise deployments) as well as those on the corporate network.

Socialite not only controls access to more than 95 features across social networks, but can also moderate, manage, and archive any social media traffic routed through the solution using either an ICAP connected or onboard proxy server for enterprise traffic or a hosted access point for those organizations using the SaaS deployment option.

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

- Identity Management – the ability to establish a single corporate identity and track users across multiple social media platforms (e.g. @JohnJones on Twitter is the same as JohnHJones on LinkedIn).
- Data leak prevention – Preventing sensitive data from leaving the company, either maliciously or inadvertently
- Granular Application Control – enabling the access to Facebook, but not access to chat, or downloading and installing any of the applications in the gaming category.
- Moderator control – for Facebook, LinkedIn and Twitter, where content is required to be pre-approved by a Corporate Communications Officer or other third party.
- Activity control – the ability to manage access to features, such as who can read, like, comment upon or access 95 features.
- Log conversation and content – capture all posts, messages and commentary made to Facebook, LinkedIn and Twitter – in context; Including exporting to an archive of choice for eDiscovery.

Ten Steps to UC, IM and Web 2.0 Compliance

1. **Gain visibility of 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 usage policy will let users know exactly what they can and can't do using UC, IM and Web 2.0 applications. Don't forget to include that the organisation has the right to monitor all traffic and to remind RRs 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 particular real-time application or social networking sites, without monitoring in place they can never be certain that users are 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 organisations block certain file types such as only the marketing department can receive gifs and jpegs, consider limiting the various types of real-time communication via job function.

5. **Apply policy management and control**
   Apply centralized policy management and control with a single solution for setting and enforcing policy for all elements of Web browsing, UC and IM in use in the enterprise. Use Active Directory integration to set global, group, user 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 communication tools such as Skype can be monitored and blocked where necessary.

7. **Implement Ethical Walls**
   Prevent RRs from accidentally meet conflicting personnel within official chatrooms.

8. **Use Disclaimer Messages**
   Customizable disclaimer 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 prove a point on compliance or just to confirm a contractual change, 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 uncover existing endpoint infections when the spyware starts trying to 'phone home'.

About FaceTime

FaceTime Communications enables the safe and productive use of Unified Communications and Web 2.0, including social networks, blogs, and instant messaging. Ranked number one by IDC for five consecutive years, FaceTime's award-winning solutions are used by more than 1,500 customers for the security, management and compliance of real-time communications. FaceTime supports or has strategic partnerships with all leading public IM network and Unified Communications providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM and Cisco.

FaceTime is headquartered in Belmont, California.

More Information

For more information about FaceTime Communications and FaceTime solutions please visit http://www.facetime.com.

Worldwide Headquarters
1301 Shoreway, Suite 275
Belmont, CA 94002 USA
(650) 631-6300 *phone*

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

APAC Headquarters
1 North Bridge Road
High Street Centre #22-07
Singapore 179094
+65 6527 2230 *phone*