
The Impact of New Communications Tools for Financial Services Firms

**by
Michael Osterman
Osterman Research**

Published September 2009

**sponsored by
FaceTime Communications
www.facetime.com**

Why You Should Read This White Paper

Securities traders, banks, investment advisors and others in the financial services industry have long embraced new communication tools. Email, for example, and more recently instant messaging can provide individuals within these firms with a distinct competitive advantage by providing information more quickly or allowing them to make more well-informed decisions. Regulators, such as the Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), the Financial Services Authority (FSA) and others have established regulations regarding the appropriate use and management of the content generated using these tools.

However, like businesses in virtually all other industries, financial services firms want and need to use new communication and information tools to supplement their use of more traditional technologies. These tools include unified communications systems that integrate email, real-time chat and voice into a single platform; social networking tools like Twitter, Facebook and LinkedIn that permit dissemination and gathering of information in novel ways; Skype, that combines traditional telephony with presence-based capabilities; and other tools. Those in the financial services industry can gain significant competitive advantage and make decisions more quickly through the use of these tools.

However, there are significant risks associated with improper use of these technologies. A financial services firm that does not manage its use of these tools properly can put itself at serious risk of non-compliance with governmental and other regulatory authorities resulting in heavy fines; it can seriously damage its reputation; and it can lose customers. Add to all of this the fact that the current recession – and its underlying causes – are giving regulators around the world more reason to focus heavily on governance of financial institutions at every level.

WHAT SHOULD YOU DO?

Any organization in the financial services space should do two things with regard to use of new communication and information technologies:

- Use them, since they can provide competitive advantages, lower costs and allow an improved level of customer service...
- ...but manage them properly, making sure to follow industry and regulatory best practices for logging content, blocking threats, preventing data leaks, archiving content and controlling their use.

ABOUT THIS WHITE PAPER

This white paper discusses some of the newer technologies in use by financial services firms, some of the variety of regulations imposed upon these firms, and offers advice on what organizations should do to mitigate the risks created by use of new communication technologies. It also discusses the sponsor of this white paper, FaceTime, and its new offerings that specifically address the issues addressed in this document.

Communications in the Financial Services Industry

GROWING ADOPTION OF UNIFIED COMMUNICATIONS

Both voicemail integration and enterprise instant messaging hold up the promise of speeding up business processes and streamlining communication between people, particularly in the financial services industry. Voicemail integration with email inboxes means that end users can get their voicemail from wherever they get email, thus eliminating voice messages as a separate and siloed place. Enterprise instant messaging, when combined with presence, gives a clear indication of when people are available for interaction, irrespective of their location or time zone.

Instant messaging plays a critical role in the financial services industry and it has for years. For example, the Financial Services Instant Messaging Association – formed by seven financial services firms – was founded in 2002 and reflected the early adopter nature of financial services firms in the context of instant messaging. As further evidence of the important role of instant messaging in the financial services industry, in June 2003 the NASD (now FINRA) required regulated financial services firms to archive their relevant instant messaging conversations just as they archive emails.

There are a variety of problems associated with managing messaging systems, real-time communications systems, such as instant messaging; as well as unified communications, social networking and the like. As shown in the following table, organizations face a variety of problems in this regard.

Seriousness of Various Management Problems
% Responding a Serious or Very Serious Problem

Problem	%
Compliance with email privacy regulations	31%
Virus, worm, Trojan, other malware infections	31%
Spyware infections	31%
Phishing attacks	30%
Personal use of instant messaging	29%
The lag between new virus outbreaks and when our AV vendor issues an update to deal with these outbreaks	28%
Users working at home creating security problems	28%
Data loss from employees sending confidential info via instant messaging	24%
Denial-of-service attacks	23%
Spam over instant messaging (SpIM)	23%
Use of consumer instant messaging clients creating security problems	22%
Reliance on public instant messaging	20%
Local/regional targeted attacks	17%

Skype is another important service that is finding more business users, including those in the financial services industry. For example, as of Q1/2009, there were 443 million total Skype accounts with 42.2 million users on a typical day¹.

SOCIAL NETWORKING TOOLS ARE BECOMING IMPORTANT

Social networking tools are exploding in popularity. Consider the following:

- Facebook has 250 million users, LinkedIn has 45 million and Twitter has 30 million.
- Nielsen released a report on June 2, 2009 that showed users spent a total of 13.9 billion minutes on Facebook during April 2009, 300 million minutes on Twitter and 202.4 million minutes on LinkedIn.
- During the one-year period ended April 2009, Facebook experienced an increase in time spent on the site of 699%².

While users of social networking sites are primarily consumers, there is growing use of social networking for a wide range of business purposes, including marketing, public relations and general business communication. For example, a growing number of banks are using Twitter for marketing purposes, to update customers about new offerings, and for other purposes. As of late August 2009, a large number of banks have a Twitter presence, including Wells Fargo, North Shore Bank, 1st Mariner Bank, Arvest Bank, RBC Royal Bank, Fidelity Bank and Peoples State Bank, to name just a few of the growing number of financial institutions with a presence on Twitter. All of the communications from these organizations is potentially subject to public (read SEC) scrutiny and must be stored and reviewable.

Further, use of social networking in a business context is not limited to younger people as many believe: an Osterman Research survey conducted in July 2009 found that the median age of business-focused Twitter users is 40 years³.

Twitter is currently used by many in the financial services and commodities industries to share articles, comments and other information. While social networking is rarely used to transmit information about trades per se, it is used to share information that can directly relate to trades. For example, a commodities trader with a network of farmers she follows on Twitter can receive non-public information that may be directly useful to her as she considers future trading opportunities. A financial analyst can discuss his opinion on certain companies or events, albeit with the proviso that tweets can be considered a form of advertising and, hence, subject to regulatory requirements for supervisory review.

It is also important to understand that FINRA's rules apply not only to traditional modes of communication like email, but also to newer tools like social networks and blogs. For example, the blog posts or Tweets of a registered individual that acts as a representative of his or her company must preserve and disclose this content just like advertising and sales

¹ <http://ckipe.com/borderless>

² http://money.cnn.com/2009/06/02/technology/social_network_growth/

³ *Results of a Survey on Twitter Usage*, Osterman Research, Inc., July 2009

literature must be preserved. This problem is exacerbated when using publicly available blogging or social networking tools that may not always be available.

Perhaps no industry will benefit more from the use of social networking than the financial services industry, particularly in light of the economic downturn that began in December 2007. Arguably, a key contributor in bringing about the current financial downturn was a lack of information and a general lack of transparency about credit markets, the housing market, the state of various financial institutions, the SEC's investigatory acumen, etc. It may be that in the future the use of social networking tools will facilitate the sharing of information in ways that could alert investors and others earlier than they can be alerted today, yielding more and better information with which to avert some of the problems in which we find ourselves now.

The Growing Risk of Non-Compliance

REGULATIONS GOVERNING UC, IM AND SOCIAL NETWORKING

There are a large number of regulations that govern data breaches and archiving and – by implication – how unified communications, instant messaging and social networking tools can and should be used. Among the more important of these regulations are the following:

- **Gramm-Leach-Bliley Act (GLBA)**

The Gramm-Leach-Bliley Act requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule (16 CFR Part 313) and the Safeguards Rule (16 C.F.R. Part 314). The wide-ranging Safeguards Rule mandates what companies should include in their written information security plan and how to secure this information, including using tough-to-crack passwords and encrypting sensitive customer information when it is transmitted electronically via public networks. GLBA also addresses steps that companies should take in the event of a security breach, such as notifying consumers, notifying law enforcement if the breach has resulted in identity theft or related harm, and notifying credit bureaus and other businesses that may be affected by the breach.

The impact of GLBA on Web 2.0 tools and technologies is substantial. It requires that the content of communications be monitored for sensitive content that should not be sent in clear text, such as personally identifiable credit information; as well as content that should never be sent via public communications channels, such as Twitter.

- **Federal Rules of Civil Procedure**

The FRCP are a body of rules focused on governing court procedures for managing civil suits in the United States district courts. While the United States Supreme Court is responsible for promulgating the FRCP, the United States Congress must approve these rules and any changes made to them. A number of important and substantive revisions to the FRCP went into effect on December 1, 2006. These changes represented several years of debate at various levels and will have a significant impact on electronic discovery

and the management of electronic data within organizations that operate in the United States. In a nutshell, the changes to the FRCP require organizations to manage their data in such a way that this data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.

The FRCP requires the preservation of business records in whatever medium they may have been produced or stored. This means that email and instant messaging conversations must be preserved for long periods if they contain material that a court or party to a legal action might deem to be discoverable. It also means that posts to social networking sites and other venues must be preserved if the content might reasonably be determined to be discoverable at some point.

- **Privacy of Consumer Financial Information (Regulation S-P)**

Regulation S-P has been adopted by the US Securities and Exchange Commission (SEC) in accordance with Section 504 of the GLBA. This section requires the SEC and a variety of other US federal agencies to implement safeguards to protect non-public consumer information, and to define standards for financial services firms to follow in this regard. The rule applies to brokers, dealers, investment firms and investment advisers.

As with the GLBA requirements noted above, sensitive content must be protected so that it cannot be intercepted by unauthorized parties.

- **SEC and FINRA Rules**

Members of national securities exchanges, brokers and dealers are obliged to preserve all records for a minimum of six years, the first two years in an easily accessible place (SEC Rule 17a-4). The affected records are broad and encompass originals of communications generated and received by individuals within financial institutions, including inter-office memoranda and internal audit working papers. Also included are automated messages sent to all customers, which could include email blasts. The records may be "immediately produced or reproduced on 'micrographic media' [microfilm, microfiche or similar] or by means of 'electronic storage media'.

FINRA is a non-governmental regulator formed in 2007 by the merger of various functions of the New York Stock Exchange and the National Association of Securities Dealers. FINRA manages a wide variety of rules that are imposed upon the more than 5,000 brokerage firms and nearly 675,000 registered representatives it oversees. Rule 3010 requires that relevant securities dealers' correspondence with the public must be supervised, reviewed and retained. The goal of NASD 3010 is to ensure that registered representatives are not making inappropriate claims to their customers, such as sending an email to a customer that guarantees that a stock will increase in value.

The impact of SEC and FINRA requirements on those who employ Web 2.0 tools and technologies should not be underestimated. There has been a requirement to preserve email communications for many years and instant messaging conversations since June 2003. The SEC and FINRA are extending existing rules governing the retention of electronic data to newer technologies, such as social networking, without creating explicit rules that specifically address these tools, meaning that all electronic content must be preserved in accordance with long-standing rules for data retention. Further, as

noted later in this report, seemingly innocuous content like recommendations on LinkedIn are treated as testimonials and are governed by SEC rules.

- **Payment Card Industry Data Security Standard**

The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers' and others' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

The four levels of PCI DSS compliance are Level 1 (any merchant processing more than six million transactions or that has suffered a data breach), Level 2 (merchants processing between one and six million transactions annually), Level 3 (merchants processing between 20,000 and one million transactions annually) and Level 4 (merchants processing under 20,000 transactions annually).

PCI DSS requirements impose a significant burden on any organization that uses electronic communication or Web 2.0 technologies. Sensitive and confidential data must be protected from interception by unauthorized parties, requiring the use of encryption and other safeguards.

- **Red Flag Rules**

Part of the Safeguards Rule, the Red Flag Rules requires financial institutions and creditors to implement a program to detect, prevent, and mitigate instances of identity theft. Affected businesses must develop and implement written identity theft prevention programs, which were required to be in place by Nov. 1, 2008. The programs "must provide for the identification, detection, and response to patterns, practices, or specific activities – known as 'red flags' – that could indicate identity theft."

As with other possible venues for identity theft, Web 2.0 technologies like instant messaging and social networking tools must be protected from malware that could allow hackers and other criminals to obtain confidential information. Given that social engineering techniques are particularly effective with Web 2.0 tools because of the implied trust that many users have in them and the supposed integrity of their contact lists, organizations must take strict precautions to protect these tools from the growing variety of malware directed against them.

- **Sarbanes-Oxley**

The Sarbanes-Oxley Act of 2002 requires all public companies and their auditors to retain such relevant records as audit workpapers, memoranda, correspondence and electronic records – including email – for a period of seven years. Company officers are obliged to report internal controls and procedures for financial reporting and auditors are required to test the internal control structures. Businesses have to ensure employees preserve information – whether paper- or electronic-based – that would be relevant to the company's financial reporting.

As with the FRCP requirements noted above, organizations must preserve relevant content from Web 2.0 tools, including things like instant messaging conversations

between corporate officers and external auditors, or even posts to social networking sites if they contain content that a regulator might deem to be a business record.

- **CSA NI 31-303**

Canadian Securities Administrators National Instrument 31-303 requires broker-dealers, registered representatives, and certain other employees of banks and other financial institutions to maintain adequate records for a variety of transactions and other communications. Records must be kept for two years in a manner that allows rapid delivery to a regulator, and for a total of seven years from the implementation of the Act.

- **IDA 29.7**

The Investment Dealers Association of Canada (IDAC) has published a Guide to Record Retention Requirements that requires that “any documents which would be necessary to defend an action against a Member or support an action by a Member should be kept at least until the appropriate limitation period has expired.” Some provinces, such as Ontario and Quebec, have differing legal requirements. IDAC recommends that its members err on the side of caution and use a seven-year retention period for certain types of documents. For example, IDAC recommends that correspondence with customers be retained for seven years from the date that a customer’s account is closed.

IDAC By-Law 29.7, for example, contains a number of provisions, including the requirement to develop policies and procedures for the review of correspondence related to its business activities, retention of correspondence for five years from the date of creation, the assignment of a senior officer to be responsible for ensuring compliance with the by-law and other requirements.

As with SEC and FINRA requirements in the United States, the two Canadian requirements noted above demand the retention of relevant business correspondence and records regardless of the medium in which they were created or stored. This means that email, instant-messaging conversations, posts to social networking sites and other content must be retained and managed in such a way that it can be produced on demand.

- **Universal Market Integrity Rules (UMIR) Policy 7.1**

This requirement focuses on the obligations of investment dealers. A key provision in UMIR is that “the compliance procedures of the [investment dealer] should allow the [investment dealer] to take into consideration, as part of its compliance monitoring, information which the [investment dealer] has collected respecting accounts at other dealers as part of the completion and periodic updating of the ‘New Client Application Form.’”

- **Markets in Financial Instruments Directive (MiFID)**

MiFID is a statute designed for financial services organizations operating in any of the 30 states of the European Economic Area. It is the successor to the Investment Services Directive and includes a number of provisions designed to protect the integrity of financial transactions, including transparency of transactions and the types of information that must be captured when clients place trades.

It is important to note that MiFID specifically requires instant messaging conversations to be retained when trades are referenced. However, it is also a best practice to preserve content from other Web 2.0 applications, including social networking tools.

- **Financial Services Authority**

Senior Management Arrangements, Systems and Controls (SYSC) 3.2.20 in the FSA Handbook has three key provisions that are relevant for organizations using unified communications, instant messaging and related tools:

1. A firm must take reasonable care to make and retain adequate records of matters and dealings (including accounting records) that are the subject of requirements and standards under the regulatory system.
2. Subject to (3) and to any other recordkeeping rule in the Handbook, the records required by (1) or by such other rule must be capable of being reproduced in the English language on paper.
3. If a firm's records relate to business carried on from an establishment in a country or territory outside the United Kingdom, an official language of that country or territory may be used instead of the English language as required by (2).

Other relevant provisions from the FSA include:

- SYSC 9.1.1 - A firm must arrange for orderly records to be kept of its business and internal organisation, including all services and transactions undertaken by it, which must be sufficient to enable the FSA or any other relevant competent authority under MiFID to monitor the firm's compliance with the requirements under the regulatory system, and in particular to ascertain that the firm has complied with all obligations with respect to clients.
- SYSC 9.1.2 - A common platform firm must retain all records kept by it under this chapter in relation to its MiFID business for a period of at least five years.
- SYSC 9.1.5 - In relation to the retention of records for non-MiFID business, a firm should have appropriate systems and controls in place with respect to the adequacy of, access to, and the security of its records so that the firm may fulfill its regulatory and statutory obligations. With respect to retention periods, the general principle is that records should be retained for as long as is relevant for the purposes for which they are made.
- Policy Statement 08/1 – Telephone Recording: recording of voice conversations and electronic communications (Sections A1.64 through A1.72). This policy statement focuses on the use of public and enterprise instant messaging solutions, the need to record conversations using these systems, and the FSA's conclusion that a solution that was presented to them was compliant with their requirements.

FSA requirements on the use of Web 2.0 tools and technologies are fundamentally no different than those imposed by SEC, FINRA or other rules: data must be retained for long periods and made available in a form that is required by regulators.

- **Model Requirements for the Management of Electronic Records (MoReq)**
MoReq, originally developed in 2001, defines the functional requirements for the manner in which electronic records are managed in an Electronic Records Management System. MoReq has been used widely in Europe and has been updated with MoReq2.

What Could Go Wrong?

EXAMPLES OF WEB 2.0 GONE AWRY

While incredibly useful in the financial services industry, Web 2.0 tools can be used in ways that could cause enormous harm to an organization. Examples include:

- During 2007 and 2008, an employee of Société Générale, Jérôme Kerviel, used instant messaging to manage fraudulent trades made on behalf of his employer, resulting in the loss of roughly €4.9 billion for the French bank. This was the second largest banking fraud ever discovered.
- The nasal spray form of cold remedy Zicam, produced by Matrixx Initiatives, has potentially been found to damage some peoples' sense of smell. This news was first revealed in Twitter discussions on June 15, 2009, resulting in a drop in Matrixx' stock price from \$19.24 that day to \$5.78 on June 16th. The stock has not been higher than \$6.55 since that time.
- While 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 his or her LinkedIn page.

THE CONSEQUENCES OF NON-COMPLIANT SECURITY AND RETENTION

There are a number of consequences arising from a failure to comply with the various obligations to retain instant messaging conversations, emails and other relevant content. Among the more serious of these problems are fines – sometimes quite substantial – as shown in the following examples:

- James B. Nutter & Company reached a settlement with the Federal Trade Commission regarding the former's failure to meet minimum federal information security standards under GLBA⁴. The company must submit to five security audits during a 10-year period as a result.

⁴ <http://is.gd/2xFjI>

- Centaurus Financial, Inc. was fined \$175,000 by FINRA for its failure to protect its customers' confidential information⁵.
- Merchant Securities was fined £77,000 by the FSA for its failure to implement robust security controls, for storing unencrypted customer data at an employee's home, and for failing to properly manage its employees' use of instant messaging, among other issues⁶.
- HSBC Insurance Brokers Limited and HSBC Actuaries and Consultants Limited were fined £700,000 and £875,000, respectively, for "not having adequate systems and controls in place to protect customer's confidential details from being lost or stolen"⁷.
- LPL Financial Corporation was fined \$275,000 for its failure to safeguard customer information under Regulation S-P⁸.
- Five broker-dealers were fined a total of \$8.25 million for their failure to preserve email communications. Specifically, the firms were fined for their violation of NASD Rule 3010, NYSE Rule 342 and SEC Rule 17a-4⁹.
- NYSE fined Schwab \$1 million, in part, for its failure to preserve internal instant messaging conversations and emails¹⁰.
- Fidelity Brokerage was fined \$2 million by the SEC and the NYSE for violations of Rule 17a-4¹¹.
- Woodbury Financial Services was fined \$65,000 by the SEC for not preventing registered representatives leaving the firm from taking with them non-public customer information¹².

A sample of the fines and penalties for violation of various statutes is shown in the following table.

⁵ <http://is.gd/2xOuT>

⁶ <http://is.gd/2xGwD>

⁷ <http://www.fsa.gov.uk/Pages/About/Media/Facts/fines/index.shtml>

⁸ http://www.pepperlaw.com/publications_update.aspx?ArticleKey=1244

⁹ <http://www.sec.gov/news/press/2002-173.htm>

¹⁰ <http://www.nyse.com/pdfs/05-110.pdf>

¹¹ <http://www.sec.gov/news/press/2004-103.htm>

¹² <http://is.gd/2xM9P>

**Selected Financial Services Regulations
and Associated Consequences for Violations**

Regulation	Consequences
Gramm-Leach-Bliley Act	Substantial fines, imprisonment for up to five years and likely loss of corporate reputation.
Regulation S-P	Substantial fines and likely loss of corporate reputation.
SEC Rule 17a-4	Substantial fines and likely loss of corporate reputation.
SEC Rule 203(b)(3)-2	Fines up to \$500,000, imprisonment for up to 10 years.
PCI DSS	Fines of up to \$500,000. Visa imposes a fine of up to \$50,000 for the first violation in a rolling, 12-month period, up to \$100,000 for the second violation, and refusal to accept future transactions until compliant for the third violation.
Red Flag Rules	FTC can impose a civil penalty of up to \$2,500 per violation; individual states can impose penalties of up to \$1,000 per violation.
NASD 3010	Substantial fines and likely loss of corporate reputation.
Sarbanes-Oxley	Fines up to \$1 million, imprisonment for up to 20 years and likely loss of corporate reputation.
CSA NI 31-303	Substantial fines and/or criminal prosecution.
IDA 29.7	Substantial fines and likely loss of corporate reputation.
FSA regulations	Substantial fines and likely loss of corporate reputation.

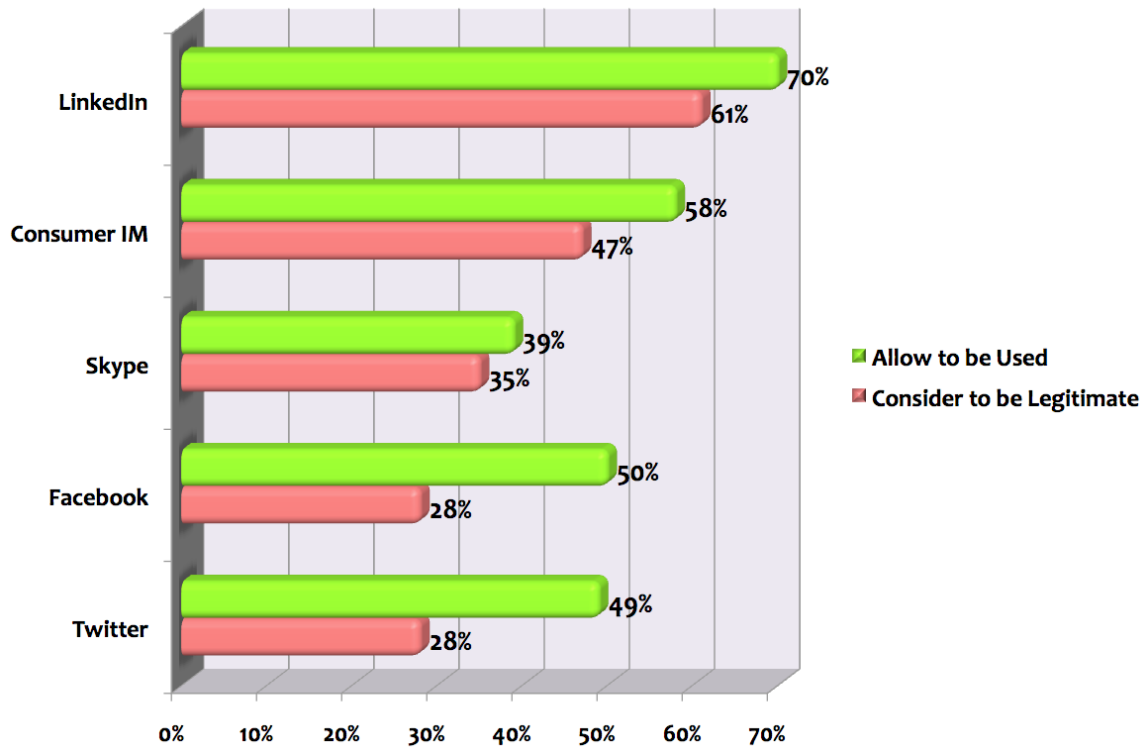
Best Practices to Mitigate the Risks

There are a variety of things that any financial services company must do in the context of managing their employees’ and others’ use of instant messaging, social networking and other tools. We have developed six basic points that every decision maker should seriously consider as they attempt to minimize the risks that their organization faces from unfettered use of these tools, while at the same time maximizing the value they can derive from them.

CONTROL USE OF UNAUTHORIZED TOOLS

An Osterman Research report published in June 2009 found that only 28% of IT decision makers consider Twitter to be a legitimate tool for use in a business context, but 49% allow it to be used in their organizations. We found a similar pattern for a variety of other tools, as shown in the following figure.

Tools Allowed and Considered to be “Legitimate”



As demonstrated in the figure above, IT departments allow far more use of communication and information tools than they consider to be legitimate, resulting in the potential for serious risk if the content from unauthorized use of these tools is not logged or otherwise managed properly. It is imperative that financial services firms implement capabilities that can control use of communication and information tools so that only authorized users can use specific tools.

LOG ALL CONTENT, INCLUDING POSTS TO SOCIAL NETWORKING SITES

It is absolutely vital to log all content sent through instant messaging clients, unified communications systems, social networking tools and Web sites, even if the use of these tools is unofficial and not sanctioned formally by either the IT department or an organization’s senior management. A failure to log traffic sent to or received from any communication or information venue can result in serious consequences with regulators, customers and others.

For example, a trader can offer his opinion on an IPO via Twitter that might be at odds with the formal position of the company or in violation of a regulatory requirement; an investment advisor might discuss the merits of investing in a stock via LinkedIn that the SEC might consider to be a regulated communication. In short, the content posted or received from any social networking, instant messaging or other tool must be logged so that an organization can a) monitor these communications for policy enforcement purposes, and b)

correct errant employee behavior, if only after the fact. However, some tools, such as Twitter, do not offer logging capabilities.

BLOCK THREATS

There are a variety of threats that can be distributed through social networking, instant messaging, unified communications and other tools. For example, an Osterman Research survey published in June 2009 found that in 15% of organizations malware had successfully infiltrated the corporate network through an instant messaging client during the one-year period ended Spring 2009. Fifty-five percent of organization had experienced malware infiltration through the Web – often through Web 2.0 applications like Twitter – during the same period.

Social networking and instant messaging tools, for example, can be used to download malware and distribute them to a large number of people rapidly. For example, a link in an instant message will often be assumed by the recipient to be valid since it was purportedly sent by a trusted source. However, if that source points to a source of malware, clicking on the link will turn the recipient's instant messaging client into a source of malware that will then attempt to infect everyone on his or her distribution list.

The key, then, is to monitor the use of all communication venues and block threats from being propagated throughout the network while allowing legitimate traffic to be passed through unencumbered.

PREVENT DATA LEAKAGE

One of the most important capabilities that any organization should enable is monitoring and preventing the leakage of sensitive, confidential or other information that could be damaging to an organization. This might include any information that is overtly sensitive, such as communication that the SEC or FINRA, for example, considers to be a regulated communication with a client. However, it can also include seemingly innocuous posts to Twitter or other social networking sites that recipients could piece together to gather intelligence about a trade, IPO or other event. The bottom line here is that sensitive information of any kind sent through any communications or information channel must be protected.

ARCHIVE CONTENT

Another critical component of any information management strategy is the ability to archive all content sent or received regardless of the tools that are used to send it. This obviously includes emails, which the SEC has required to be archived for many years; as well as instant messages, which as noted earlier, have had to be archived since June 2003.

As of this writing, there are no specific SEC, FINRA, FSA or other rules that specifically require the archiving of Twitter content or posts to other social networking sites. However, based on published reports of FINRA's position on rules for new communication technologies, it can safely be assumed that posts to Twitter or other social networking sites, or the use of Skype or unified communications tools, will be governed in much the same way as more formal communication modes like email or instant messaging. As a result, any financial

services firm must, as a best practice, archive content to or from all of these venues in order not to run afoul of future regulators' decisions.

INTEGRATE WITH EXISTING ARCHIVING SYSTEMS

Closely related to the point above is that it is imperative not only to archive content for any communication or information system, but also to integrate this archived content with existing archiving tools in the organization. Because broker-dealers and others must archive the emails sent by their registered representatives and others, it is clearly a best practice to integrate other content archives into the primary archive already used. This can save significant amounts of time when searching for content, such as in response to a regulatory audit when time is of the essence, and can ensure a common interface is used to search for and access content regardless of its source.

Summary

Financial services firms have long had to manage content in a manner that is consistent with regulators' requirements and industry best practice. This includes the traditional content medium of paper, of course, but more recently content sent electronically through email and instant messages. However, as modes of communication progress and new technologies are introduced, users in financial services firms have been presented with a growing array of new communications alternatives, including unified communications systems that can contain voice content as easily as they can contain emails or instant messaging conversations; social networking tools like Twitter, Facebook or LinkedIn; or telephony alternatives like Skype that combine voice and instant messaging capabilities.

While the regulation of these new forms of communication has not always kept pace with their use, there are a variety of reasons for organizations to embrace use of these new technologies in order to gain competitive advantage, reduce costs and provide better customer service. At the same time, however, there are a number of best practices than any financial services firm should follow to ensure that it will be compliant with current and anticipated regulations and that it will minimize the risks associated with use of these tools.

About FaceTime

FaceTime Communications enables the safe and productive use of instant messaging, Web usage and Unified Communications platforms. Ranked number one by IDC for five consecutive years, FaceTime's award-winning solutions are used by more than 1,000 customers for security, management and compliance of real-time communications. FaceTime supports or has strategic partnerships with all the leading public and enterprise IM network and unified communications providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM and Jabber.

FaceTime is headquartered in Belmont, California. For more information, visit <http://www.facetime.com> or call 888-349-FACE. The FaceForward blog at

<http://blog.facetime.com>, offers thoughts and opinions about the changing nature of Internet communications.

FaceTime Communications, Inc.
1301 Shoreway
Suite 275
Belmont, CA 94002
USA

Toll-free: +1-888 349 FACE (3223)
Phone: +1 650 631 6300
Fax: +1 650 598 2820
info@facetime.com

For Web and Unified Communications security news follow FaceTime on Twitter,
<http://www.twitter.com/facetime>

© 2009 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.