



Best Practices for Emerging Compliance Challenges: Electronic Messaging & Communications

Prepared By:

Julie Olson
Senior Consultant
ReymannGroup, Inc.

“With the increased privacy and security awareness among businesses, customers, and our elected officials, traditional best practices are being incorporated into new laws and regulations that define a higher security standard that all affected organizations must achieve. Information security is no longer only a prudent business decision, it is mandated!”

This paper highlights IM and P2P compliance best practices your organization should consider.

Sponsored By:

FaceTime™

CONTENTS

Evolution of Communication Practices and the Growth of IM and P2P	3
Emerging Laws and Rules <ul style="list-style-type: none">• FDIC IM Guidance• SEC Rules• NASD Requirements• NYSE Requirements• Sarbanes-Oxley Act• Gramm-Leach-Bliley Act• HIPAA• Others	4
Compliance “Best Practices” <ul style="list-style-type: none">• Blocked File Sharing• Authorized Use Policy• Restricted Access to Sensitive Data• Authentication• Non-repudiation• Confidentiality of Data• Monitoring & Auditing• Secure Logging and Audit Trails• Tamper Proof Environments• Content Scanning & Keyword Matching• User Awareness	7
Future Compliance Issues	10
Next Steps Towards Compliance <ul style="list-style-type: none">• Self-assessment Checklist	10

EVOLUTION OF COMMUNICATION PRACTICES

Information security issues were present even in the days of stage-coach mail delivery, but they were relatively simple to resolve — put an armed guard on top of the stage coach and make those horses run like lightening! Today’s information sharing methods have evolved since the days of stage coach delivery with telegraph exchange, paper mail delivery, party-line and private-line telephone calls, and bulletin board messages, to innovative methods such as e-mail and more recently, instant messaging (IM)¹ and peer-to-peer (P2P)² file sharing. Over time, all of these methods advanced the speed and ease of information exchange, and created new challenges for securing, managing, and controlling the content and use of information.

In the early years of the telephone, party lines were the norm, and no one worried too much about who might overhear that your sister was getting married or that the neighbor’s were getting new furniture. It was common for neighbors to know what was going on in their neighborhood through the use, and sometimes perhaps abuse, of the party line. Today, businesses, individuals, and governmental entities cannot afford to be passive about who might be eavesdropping on their conversations or business transactions.

The more recent evolution to the use of e-mail, IM and P2P by individuals and businesses has presented especially difficult challenges in keeping proprietary business or customer information safe and secure. These new communication mediums have grown quickly and are definitely here to stay. The *Wall Street Journal* recently stated that IM is now the fastest growing form of IP-based communications, and Osterman Research estimated that 90 percent of all businesses in North America use IM to some extent. The Gartner Group expects that IM will surpass e-mail as the preferred form of electronic communication by 2006. Additionally, multiple market analyst firms estimate that IM will reach e-mail penetration levels by the end of 2006, emphasizing that the popular P2P program Kazaa has been downloaded over 300 thousand times.

Clearly, employee use of IM and P2P communication mediums is on the increase in most companies. Ready or not, your company must assure that it is prepared to manage the security and compliance risk that accompanies such mediums. There are a growing number of laws and regulations regarding recordkeeping and the use and security of non-public information that many businesses must follow. These laws apply regardless of the medium used to transact communications. No business today can afford to have its reputation diminished because it did not properly comply with government mandates or because it failed to adequately protect its confidential customer information. Public IM and P2P messaging are open communication channels. This makes them especially vulnerable to security breaches and susceptible to viruses, worms, phishing³ techniques and transmission interceptions.

¹ Webopedia, an online computer technology encyclopedia, defines IM as a communication service that enables a user to create a kind of private chat room with another individual to communicate in real time over the Internet. Generally, this type of communication travels from the sender to the IM’s server and then to the recipient of the message.

² Webopedia defines peer-to-peer (P2P) as a type of network in which each workstation has equivalent capabilities and responsibilities. P2P networks can either use servers to direct traffic or directly connect desktops over an IP network. While P2P communication was initially used to share soundtracks, businesses have begun to use it to take advantage of the computing power they already own.

³ Criminals are using “phishing” to illegally obtain personal information and perpetrate identity theft. The criminals transmit e-mails and IM to trick unsuspecting individuals into believing they are communicating

Companies that allow employees to use public IM or P2P messaging should also be aware of the risk involved if employees download files that are subject to copyright laws and rules. As an example, in 2002 the recording industry agreed to a \$1 million settlement with an Arizona company that allegedly allowed employees to trade copyrighted MP3 files over a dedicated server. In addition, these electronic means of information sharing are especially tempting for employees' personal use, which can waste company time and expose confidential company and customer information to unauthorized outside access.

With the increased workplace use of IM and P2P, ReymannGroup has authored this white paper to summarize the regulatory, business, operational and technology risks companies face and offer corrective measures and compliance best practices that management can use to address the risk and control the use of these new communication mediums.

EMERGING LAWS AND RULES

The reliance of today's industries and businesses on the use of electronic messaging and communication makes information security paramount. Prudent management of any organization that depends on the confidential use and transmission of sensitive information must incorporate industry recognized and regulatory mandated best practice techniques to ensure confidentiality and adequate recordkeeping. All organizations **MUST** have clear policies and procedures for the proper use or enforced blocking of all messaging and communication methods, including IM and P2P communications.

With numerous and constant security threats to electronic messaging and communication channels, many businesses and individuals have developed methods to address these threats. Over time, those methods that work well have evolved into industry best practices. Many of the best practice techniques for identifying and controlling such risks have evolved from organizations that recognized their exposure early. They took proactive steps to act – not because there was a law or rule mandating such steps – but as good business practice to protect the organization, its employees, and customers.

Now with the increased privacy and security awareness among businesses, customers, and elected officials, traditional best practices are being incorporated into new laws, regulations and supervisory guidance that define a higher security standard that all affected organizations must achieve. Information security is no longer only a prudent business decision, it is mandated.

Companies that are publicly traded, financial service providers, health care providers, and many other businesses must comply with a number of new laws and supervisory guidance. Such mandates include:

- **FDIC IM Guidance** – In late July 2004, the Federal Deposit Insurance Corporation (FDIC)⁴ issued guidance to all insured depository institutions on the risks associated with the use of IM. These risks are not limited to financial services; the guidance is useful to any company using or considering the use of IM or P2P communications.

with a legitimate enterprise to confirm or update information such as passwords, bank account numbers, social security numbers, or credit card numbers.

⁴ See FDIC Financial Institution Letter FIL-84-2004: Guidance on the Risks Associated with Instant Messaging. See also www.fdic.gov.

- SEC Storage of Broker Dealer Records (a.k.a., Recordkeeping Rules) –17 CFR Parts 240 and 242: Books and Records Requirements for Brokers and Dealers under the Securities Exchange Act of 1934⁵ require Members of a national securities exchange who transact a business in securities to keep current books and records relating to its business, including recordkeeping of certain communications.
- NASD Guidance – The NASD has issued an Internet Guide for Registered Representatives⁶ that includes guidance on all communications, including the use of IM. This guidance provides information on NASD rules affected by the use of IM.⁷
- NYSE Rules – The NYSE includes rules that guide members in retaining communications with the public that must comply with Rule 440 (Books and Records).⁸
- Sarbanes-Oxley Act of 2002 (SOX)⁹ – The intent of this Act is to protect investors from inadequate or inaccurate corporate disclosures. All publicly traded companies must comply with SOX. The Act required the SEC to establish auditing and quality control standards for public accounting firms and their clients. The SOX standards include management controls over the use of sensitive information, its storage, and its transmission.
- Gramm-Leach-Bliley Financial Modernization Act of 1998 (GLBA)¹⁰ – The GLBA requires all financial institutions to establish safeguard measures to protect data and the security and confidentiality of customer’s confidential information. GLBA holds financial institutions responsible for protecting customer records against unauthorized access and provides guidelines for the authorized use of confidential customer information.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)¹¹ – HIPAA requires covered healthcare entities to establish safeguards to protect the privacy of consumers’ health care information.

Various other laws contain provisions that also cover the use and protection of private customer information, such as:

- Various state laws that require specific protections needed due to the computerized collection of customer information.¹²
- The USA PATRIOT ACT of 2001¹³
- The Fair Credit Reporting Act of 1970.¹⁴
- The Privacy Act of 1974.¹⁵
- The Cable Communications Policy Act of 1984.¹⁶

⁵ § 240.17a-3. For further information see also www.sec.gov.

⁶ See www.nasdr.com; Internet Guide for Registered Representatives issued.

⁷ See also NASD Conduct Rule 3010; NASD Notice to Members 03-33; Notice to Members 99-03; NASD Conduct Rule 3110; NASD Rule 2211; and NASD Conduct Rule 2210.

⁸ See www.NYSE.com.

⁹ For more information on SOX visit www.sec.gov/spotlight/Sarbanes-Oxley.

¹⁰ See Public law 102-106.

¹¹ For more information on HIPAA visit www.cms.hhs.gov.

¹² For example, see CA SB 1386 Enacted 2002.

¹³ See Treasury News from the Office of Public Affairs, February 26, 2002, PO-1044 for more information on the USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001).

¹⁴ See 15 USC 1681 or visit www.ftc.gov.

¹⁵ See 5 USC 552a or visit www.usdoj.gov.

- The Electronic Communications Privacy Act of 1986.¹⁷
- The Children’s Online Privacy Protection Act of 1998.¹⁸
- Food and Drug Administration Rules.¹⁹

These legal mandates require organizations to maintain the confidentiality of sensitive information. The growing number of laws and regulations that mandate effective electronic security steps make management and control critical to any business that plans to allow the use of electronic messaging and communication tools in conducting business.

Compliance with these new security mandates can benefit an organization through:

- Continued growth of revenues.
- Protection against financial and reputation loss.
- Efficient business continuity.
- Proactive regulatory compliance.
- Protection from loss of intellectual property.

Alternatively, the noncompliance penalties can be staggering and vary from:

- Loss of corporate charter or license.
- Payment of fines and civil money penalties.
- Disbarment from an industry.
- Possible imprisonment.

For example, there are numerous cases of fines imposed that serve to emphasize the critical nature of complete and adequate electronic records management including:

- Five broker-dealers were fined \$1.65 million each because “back-up of electronic records does not constitute a retention policy” and “retention without accessibility” does not guarantee that records can be retrieved;
- A major telecommunication company was fined \$25 million for failure to cooperate with regulators. Such failure included “incomplete document production”...and failure “to ensure that a relevant document was preserved and produced;”
- The SEC recently censured a securities firm for failing to produce documents and e-mails during a pending investigation; and
- The Federal Energy Regulatory Commission (FERC) fined a major integrated, energy company a \$25 million one-time charge and required the company to sell electricity generated from one plant at cost for a 12-month period.

Another class of emerging regulations, led by the Sarbanes-Oxley Act of 2002 (SOX), increases the risk to publicly traded companies well beyond fines. Chief Executive Officers and Chief Financial Officers now face possible incarceration if convicted of records manipulation. In today’s regulatory climate, these laws could change the former ROI acronym from “Return-on-Investment” to “Risk-of-Incarceration.”

¹⁶ Public Law 98-549.

¹⁷ Public law 99-508. For more information visit www.ftc.gov.

¹⁸ 15 USC 91.

¹⁹ See FDA 21 CFR Part 11.

KEY COMPLIANCE “BEST PRACTICES”

All organizations that use IM and P2P communications face a number of emerging risks and challenges in protecting sensitive, non-public information. The operational, reputation, and regulatory vulnerabilities that electronic commerce and communications can create - if not properly managed - make it extremely important for businesses, governments, and individuals to take an active role in maintaining the confidentiality of sensitive information.

The ReymannGroup has identified several compliance best practices to help manage such risks and challenges in today’s highly regulated environments. Companies that lack an adequate risk management strategy that includes these or other similar practices could face noncompliance penalties including monetary fines.

Block All P2P File Sharing.

Until there are business justifications for P2P file sharing along with adequate management solutions to ensure that security and policy requirements can be met, companies should have their IT departments and security personnel block all P2P file sharing. Examples of P2P applications include Kazaa, Morpheus, LimeWire, etc.

Adopt an Authorized IM Usage Policy.

When employees use IM to share information, management must be certain that the employees are following an authorized usage policy defined for these methods of communication. The company usage policy should specify authorized:

- Usage policies for IM, including who can use it and what IM networks are allowed.
- Types of information that can be transmitted over such channels. For example, companies should specify certain rules for sending and receiving sensitive information through IM, including rules relating to when or if attachments can be sent.
- Awareness of key words and phrases that should be blocked or restricted including an updated list of words and phrases.
- Awareness and technical limitations to enforce “ethical boundaries” or Chinese walls between certain organizations.

Restrict Access to Sensitive Data.

Each organization using IM should have controls in place to restrict access to sensitive information on a “need to know” basis. This limits access to only authorized individuals. In transferring non-public information, companies must make sure the sensitive information is protected from unauthorized interception and that the intended recipient can be verified upon delivery of the message or transfer of data. Common best practices for such controls include the adoption of enterprise IM monitoring and IM specific identity management products. Companies should also be capable of actively auditing all information that is transferred through IM channels.

Authenticate.

Companies should institute authentication methodologies to ensure that information transmitted is sent only by those authorized and received by only those intended to receive it. Tools for IM

identity management are offered by various IM security and management vendors that can be used to authenticate the sender or receiver of information. Some information, such as files exchanged through IM, may go through an unknown server and may be subject to unauthorized access because the server is outside the control of the parties using IM. Such exposure makes it extremely important that management be aware of the mode of transmission and have the ability to block unauthorized transmissions with an IM management solution.

Assure Non-repudiation.

Assuring non-repudiation of IM or P2P transactions is vital. Non-repudiation requires measures that will ensure that a transaction processed or information received cannot be denied at a later date. Companies should consider using methods such as digital signatures or PKI and time stamping to provide legal proof that a transaction was legitimate.

Ensure Confidentiality of Data.

Companies must ensure that the confidentiality of data is maintained. Companies should employ adequate perimeter security solutions that are application aware and can either safely enable IM or effectively block IM and P2P. Most firewalls in production today cannot assure that IM and P2P are blocked or safely enabled because they lack application awareness, and the “port agility” of these emerging applications easily circumvents firewalls. Companies should also consider employing encryption methods that allow only the intended recipient to read the information once it is sent. In most cases, it may be appropriate to use these specialized IM and P2P application aware security gateways to block certain information from being sent through IM or P2P channels.

Monitor and Audit.

Companies that allow employees to use IM must monitor and audit user activities. Monitoring and auditing are essential tools in assuring that employees are following the restrictions defined in the usage policy and that non-public information is properly protected. Most emerging regulations require that all electronic communications, including IM, are properly logged, monitored, and audited for regulatory compliance. Monitoring IM use allows the company to identify and supervise users by reviewing and annotating real-time conversations. By inserting monitoring notifications in IM sessions (commonly known as IM Disclaimers), organizations can put users on notice that their conversations can be retrieved, reconstructed, and analyzed for policy violations.

Companies that choose to safely enable IM communications, while complying with regulatory requirements, must assure that employees are following policy and compliance procedures and that IM messages are compliant. To assure that a technically savvy employee does not by-pass the policy and compliance engine, a company should employ a two-tier architecture. This two-tier architecture will include an enablement and compliance engine integrated with a blocking engine that will stop all messages if an employee bypasses the compliance and audit engine.

Use Secure-logging and Maintain and Validate Audit Trails.

Laws and rules for the confidentiality of customer information mandate that companies maintain secure logging that can be used to create an audit trail if a security breach occurs. Logging should be capable of recording communications and files transfers through any IM or P2P network and should allow a company to research and audit any IM or P2P activity. Logging

allows a company to determine who is using IM, how they are using it, and whether or not the use follows established management policies.

With the risk of employee abuse or downtime due to personal use, some companies have blocked employees from using IM, even when it would enhance business opportunities. Maintaining and reviewing activity logs, however, can provide companies with an audit trail to determine compliance with the overall policies while still taking advantage of IM communications. Additionally, companies should:

- Employ systems that log and retain IM messages in a binary format to assure that all formatting and unique “emoticons” found in IM-based communication are stored and retrievable in full context.
- Look to IM security and management solutions that treat all IM networks and solutions in a consistent manner.

With an “in-stream proxy” solution, a company can assure that all messages are logged, audited, scanned for offending content, and have disclaimers inserted in a consistent manner across all public IM networks and Enterprise IM solutions.

Establish Tamper Proof Environments.

Companies should establish a tamper proof environment that prevents logged IM or P2P conversations from being modified or deleted. All logged IM and P2P information should be stored in a format that prevents anyone from gaining access to the logs and altering or deleting them. In establishing a tamper proof environment, companies should also employ IM and P2P aware security gateway and IM management systems that integrate with leading anti-virus scanning software on all individual computers whether mobile or stationary. Companies should also ensure that all software updates are promptly executed to maintain current virus protection. IM security and management solutions that employ “check-sum” anti-tampering methods are recommended.

Employ Content Scanning and Keyword Matching.

Companies must employ security measures that can monitor communications as they are sent or received. Such monitoring should scan content by searching for key words or phrases from a hot list or pattern matching for sensitive data such as credit card numbers, social security numbers, and customer account numbers. Companies should also consider employing content scanning to make sure that employees are not sharing unauthorized information or using IM or P2P communications for personal use. Companies can monitor for this type of misuse by employing security parameters that will search on key words or phrases during transmission to provide “red flag” alerts for any suspicious transmissions. Companies may also want to block employees from using certain words or sending certain data through IM or P2P channels. For example, companies should consider proactively scanning for and blocking or flagging any transmissions that contain phrases of profanity or violence, confidential information, or other sensitive data that may expose the organization to operational, legal, reputation, or physical risks.

Raise User Awareness.

As an added measure of control, companies may want to alert employees if the system detects that they are sending or discussing confidential information or using IM or P2P communication links inappropriately. This will help remind employees of the proper use of electronic

communications. In conjunction with sending an alert, companies should make sure that employees are adequately trained in the proper use of electronic security measures.

FUTURE COMPLIANCE ISSUES

Historical and modern trends show us that, similar to earlier forms of messaging and communication, the use of new electronic communication methods such as IM and P2P are valuable tools to help each business become more efficient, communicate and share information more effectively, and maintain a competitive position within its industry. It is also certain that as new forms of messaging and communication evolve, the emerging risks and mitigating best practices and perhaps laws and regulations for these electronic messaging and communication channels will also evolve.

Forward-looking companies will not wait for government to mandate the steps they should take to secure confidential and proprietary information and use IM and P2P in a prudent and safe manner. Those that proactively develop and adopt effective policies, practices, and systems will be well positioned to leverage the latest in technology to enhance their operations, bottom line, and competitive position in a safe and secure environment. Companies that can transact business faster, more efficiently, and securely will maintain their complete edge and prosper in today's and tomorrow's environment.

NEXT STEPS TOWARD COMPLIANCE

If your company plans to use or uses IM or P2P, whether authorized or not, you should perform a self assessment to make sure appropriate best practices are in place. In the chart below, check which measures your company has adopted. All should be checked in the affirmative, or you may be putting your company and your customers at risk by allowing unmonitored use to proliferate on your corporate network.

Self-Assessment Check List

BEST PRACTICE	Instant Messaging		Peer-to-Peer	
	YES	NO	YES	NO
<i>Block all P2P file sharing?</i>				
<i>Adopt an authorized IM usage policy?</i>				
<i>Restricted access to sensitive data?</i>				
<i>Authenticated transmissions and storage of data?</i>				
<i>Assured non-repudiation?</i>				
<i>Ensured confidentiality of data?</i>				
<i>Implemented monitoring and auditing capabilities?</i>				
<i>Use secure-logging?</i>				
<i>Maintain and validate audit trails?</i>				
<i>Established a tamper proof environment?</i>				
<i>Use employee content scanning and keyword matching?</i>				
<i>Raised user awareness?</i>				
<ul style="list-style-type: none"> ● <i>Employee training?</i> ● <i>Notify users of suspicious content?</i> 				



ABOUT REYMANNGROUP, INC.

ReymannGroup, Inc. provides finance and healthcare regulatory subject matter expertise. We assist companies in evaluating their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. We provide you with "independent" high-caliber professionals, authors of regulations, and subject matter experts familiar with financial and healthcare industry regulations and best practices. Our experts will meet and exceed your business need. For more information contact or e-mail us at (410) 286-9505 or info@reymanngroup.com.



ABOUT FACETIME COMMUNICATIONS

Founded in 1998, FaceTime Communications is the leading provider of extensible real-time security and management solutions that address network and information security, regulatory and corporate compliance, and call center customer service. FaceTime's award-winning solutions are used by over 350 corporate customers, with over 50 percent of the largest global 100 financial institutions, including seven of the eight largest U.S. banks. Hundreds of customers worldwide, including Chicago Stock Exchange, Dominion Energy, NCR, Southern Company, Standard Bank London, Thomas Weisel Partners, USAS Technologies and Wachovia Securities among others rely on FaceTime solutions. FaceTime has strategic partnerships with all leading public and private IM network providers, including AOL, Microsoft, Yahoo!, IBM, Bloomberg, Jabber and Reuters. FaceTime is headquartered in Foster City, California. For more information on FaceTime, visit <http://www.facetime.com> or call 888-349-FACE.