

Email Encryption Responsibilities For Financial Institutions

This paper explores some of the laws and regulations that Congress and the regulators have adopted that govern the use of electronic communications. It also provides financial institutions with information on how they can leverage encryption to be proactive in helping to maintain the confidentiality of nonpublic information when it is transmitted via electronic mail.

FEBRUARY 2005



PREPARED BY:

- > **Paul Reymann**
CEO, ReymannGroup, Inc.
- > **Julie Olson**
Financial Services
Regulatory Consultant
ReymannGroup, Inc.
- > **Sponsored By:**
Zix Corporation

TABLE OF CONTENTS

Privacy Challenges of Electronic Communications..... 3

Laws and Rules Governing the Security of Nonpublic Information..... 4

Compliance Best Practices..... 6

ZixCorp Solutions 6

NEXT STEPS – Compliance Self-Assessment 9

About..... 9

- The Authors
- ZixCorp
- ReymannGroup, Inc.

THE PRIVACY CHALLENGE OF ELECTRONIC COMMUNICATION

Prior to the electronic age, financial service providers primarily used the postal service to communicate with customers, and most communication between employees took place either over the telephone or in person. A bank would use its customer records to address an envelope and then stamp and seal it. Once mailed, banks placed their trust in the delivery mechanisms to maintain the confidentiality of the information sent. With these traditional communication and information sharing mechanisms, the bank also generally trusted employees to keep all nonpublic information private.

These delivery mechanisms were fine in the past — transactions were expected to move relatively slowly, and a loan from a customer's bank could take weeks and sometimes months to complete. Once the customer's information was obtained it was generally considered bank property, and the customer had little say over how it could be used or shared.

Today, modern financial service providers use a variety of communication channels to obtain, use, and transmit customer information, and to collaborate with customers, employees, and partners. Although they still use traditional means, most banks are turning to electronic communications such as e-mail and transactional Web sites. Bank employees are also using electronic communications to a greater extent to communicate with each other and to perform daily duties, which can frequently include the sharing of nonpublic customer information. While these new methods of communication have streamlined the gathering and sharing of information, they have also presented new challenges in making sure that information is not accessed or used by unauthorized individuals.

With the increasing use of electronic communications, financial service providers are facing evolutionary changes in the way they securely interface and communicate with customers, employees, suppliers, and partnering organizations. Transactions move faster, and customers are more aware of the need to ensure their personal information is used and protected by their banker.

Banks and other financial service providers' reputations are at risk if they are not able to assure customers they can keep their information safe and secure and that they have effective physical, administrative, and technical safeguards in place to monitor and control any unauthorized attempts to access that information. In a business where maintaining the customer's trust is vital, tools and controls that ensure security of sensitive information are essential.

While some banks may feel they are adequately protecting nonpublic information by issuing rules or policies to employees, this has provided only limited assurance that information is not subjected to the threat of unauthorized use or release. There remains the constant risk of an employee sharing or releasing private customer information, deliberately or accidentally, so that others can use it for unlawful purposes. Many banks, for example, are increasingly aware of the need to encrypt all e-mail that contains sensitive data. Policies are important, but alone they will not prevent an employee from inappropriately leaking sensitive information. The bank must supplement its internal rules and policies with effective technology solutions to assure that information is handled and transmitted securely.

Financial institution managers and directors historically have taken an active role in ensuring that they have systems and controls in place to measure, monitor, and control risks to the institution. The security of electronic communications, however, introduces some additional complexity into the risk control process. An institution that does not understand and manage the risks associated with the use of electronic mail can seriously damage its reputation if it finds it has to notify

customers of a security breach or an operational breakdown. Such occurrences could lead to costly litigation from customers or regulatory sanctions from the financial regulatory community.

As an example, in 2003, the Comptroller of the Currency (OCC) took a formal action and assessed civil money penalties against two banking officials and barred them from banking for transferring customer loan information through an e-mail attachment. The OCC charged the bankers with unsafe and unsound banking practices and for violating privacy rules by copying more than 2,200 customer loan files and e-mailing them over an unsecured Internet connection to a third party. In a press release announcing the actions, Comptroller of the Currency John D. Hawke, Jr., stated:

“National bank customers have a right to expect that the confidentiality of their financial information will be protected. The OCC will respond aggressively if we find the bank employees are misusing that information, or placing it at risk of unauthorized disclosure.”¹

This paper explores some of the laws and regulations that Congress and the regulators have adopted that govern the use of electronic communications. It also provides financial institutions with information on how they can be proactive in helping to maintain the confidentiality of nonpublic information when it is transmitted via electronic mail.

LAWS AND RULES GOVERNING THE SECURITY OF NONPUBLIC INFORMATION

Financial service providers are among the most regulated industries in the country. Many of the more recent financial industry laws and rules mandate the proper use and protection of confidential customer information. While these laws and rules cover much more than the privacy of nonpublic information, the systems and controls they mandate apply to all means of communication, including transactions conducted through electronic means. Some of the laws and regulatory guidance relevant to electronic mail for financial institutions and publicly traded companies include:

*Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA)*² – Under GLBA, all financial institutions must establish appropriate administrative, technical, and physical safeguards to protect data in transit and in storage and to maintain the confidentiality of customer’s nonpublic personal information. All institutions must evaluate the need to encrypt sensitive information and implement appropriate risk-based controls to protect against unauthorized use and distribution of that sensitive data. For example, the ability for employees to e-mail unencrypted sensitive information outside of a secure network can expose a financial institution’s operations, reputation, and compliance to risk.

*Sarbanes-Oxley Act of 2002 (SOX)*³ – SOX covers all publicly traded companies and is intended to protect investors from inaccurate corporate disclosures. The Securities Exchange Commission is charged with establishing audit and quality control standards for public accounting firms and their clients. SOX standards include management controls over the use of sensitive information, its storage, and its transmission. Electronic transmissions are covered by this Act. Such management controls also include consideration of the need to encrypt sensitive e-mails. Unauthorized exposure of confidential information can create a

¹ See OCC News Release NR 2003-27 dated April 7, 2003.

² See Public law 102-106.

³ For more information on SOX visit www.sec.gov/spotlight/Sarbanes-Oxley.

“material event” that must be rapidly and publicly disclosed. In addition to becoming a material event, the ability for employees to e-mail unencrypted sensitive information outside of a secure network can expose a publicly traded company’s operations, reputation, and compliance to risk

CA SB 1386 Enacted 2002 – California enacted Bill Number SB 1386 to require state agencies and others who conduct business through computerized collection of personal information, to expeditiously disclose any breach of data security to any California resident whose personal information may have been compromised. To meet the SB 1386 requirement, companies that conduct business in California must have effective monitoring and reporting systems to identify the unauthorized acquisition of unencrypted personal information including breaches that occur through the use of electronic mail. Companies that conduct business with California residents should consider encrypting e-mail to protect the transfer of personal customer information outside of a secure network.

Identify Theft Act of 1998 – In October 1998 Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to address the growing problem of identity theft. Identity theft can occur through a variety of means, and companies should be prepared to protect customers from unauthorized access to information that may enable a thief to obtain personal customer information. Companies that do not have a prudent security program in place to adequately protect a customer’s nonpublic information may inadvertently aide in the identity theft. If such an incident occurs and goes undetected, it will create a negative lasting affect on the company’s reputation.

The USA PATRIOT ACT of 2001 – The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 was passed to protect the Nation’s financial system from terrorist money laundering financial schemes and other acts of terrorism. This Act holds financial institutions responsible for verifying the identity of customers. Regulations implementing the Act require financial institutions that share information under the Act to take necessary steps to protect the confidentiality of the information and to use it only for the purposes specified in the rule. This means that covered institutions must assure that information sent or received electronically is protected from unauthorized use or disclosure.

Whether an institution uses manual or electronic means to transact business, management and the board of directors are responsible for making sure they have the tools in place to assure compliance with the applicable laws and rules. A list of these mandates for protecting sensitive information is included in **Exhibit 1**. Institutions that do not take these mandates seriously, or that do not institute effective tools to monitor and control the risk of unauthorized use or disclosure of nonpublic information such as the risk-based need to encrypt e-mails that contain sensitive data may be subjected to regulatory fines or civil money penalties. Some of the laws and regulations provide that the institution can lose its corporate license or charter, and officers and directors may risk being barred from working in the industry. Instituting effective compliance controls and management of nonpublic information makes good business sense – even without the laws and rules mandating it.

COMPLIANCE BEST PRACTICES

All financial institutions must institute an effective security program to manage the secure flow of sensitive information, including information sent through e-mail communications. Under GLBA, all financial institutions are required to adopt security programs that are tailored to the size, operations, and risk profile of the institution. In developing the security program, the board and management are responsible for performing a risk assessment that should include the use of electronic communications, among its other information security processes. In performing this assessment, the board and management must consider the types of information it collects, how sensitive the information is, what internal and external threats the information might face, and the risk-based control practices that are in place to mitigate those risks.

Once the risk assessment is completed, the financial institution must define the policies and procedures it expects employees to follow to protect all nonpublic information. *For example, if an institution will allow employees to send nonpublic information through e-mail, the policies and procedures should address what information can be transmitted and who is authorized to transmit it. Depending on the sensitivity of the information, management must also address the need to encrypt it during transmission to guard against unauthorized retrieval or use.* Additionally, the institution must determine how it can effectively monitor whether or not employees are following the policies and procedures in place. An institution will need to use a number of layered security measures to determine compliance and to alert appropriate security personnel if there is a breach of these policies and procedures.

An institution that does not adequately define the appropriate use and encryption of e-mail or other forms of electronic communication in its security program and risk assessment process is putting its customer information and reputation at risk. Additionally the institution could be subjected to regulatory and civil fines and other penalties if the measures do not adequately protect nonpublic customer information.

ZIXCORP CAN HELP FINANCIAL INSTITUTIONS ADDRESS E-MAIL RISKS

ZixCorp provides a proven trust model for secure communication. It offers a suite of solutions that enables financial institutions to deliver sensitive information securely and electronically to proactively maintain the confidentiality of nonpublic information. **Exhibit 1** shows how this model aligns with key regulatory mandates and best practice security policies.

ZixVPM[®] (Virtual Private Messenger) is a policy-driven, enterprise-wide solution that provides easy-to-use, easy-to-deploy e-mail encryption, content filtering, and management of inbound and outbound messages. ZixVPM also contains a Personal Financial Content Recognition lexicon that identifies e-mails containing GLBA-mandated customer financial information, including Social Security numbers, credit card numbers, account numbers, balance transfers, refinance data, and other personal financial details. ZixVPM can be easily configured to block or encrypt these sensitive e-mails according to a company's policy.

The solution can be deployed in just one day and requires very little ongoing administration. ZixVPM operates independently of existing e-mail systems and is transparent to end users. Secure messages can be sent to anyone with an e-mail address, whether they are a ZixCorp customer or not.

ZixVPM benefits include:

- Seamless integration with existing network structure
- Easy use and management while remaining completely transparent to users
- Secure communications regardless of recipient's e-mail client
- Easy customization and implementation of GLBA corporate security policies and prudent practices

ZixMail[®] is a desktop encryption solution that enables individual users to manually encrypt, decrypt, and exchange private and secure e-mails and attachments to anyone. It's an easy-to-use tool that integrates with network infrastructures, today's most popular e-mail systems, and all other offerings in the ZixCorp suite of eSecure services.

ZixMail is available as a standalone application or as an integrated part of a desktop system. With third-party time stamping and strong authentication, all ZixMail messages can provide irrefutable proof of delivery and receipt and secures both internal and external communications.

ZixAuditor[®] is a comprehensive e-mail assessment service that enables companies to identify e-mail vulnerabilities, implement more effective policies and procedures, and monitor ongoing communications to determine compliance and effectiveness. The service helps manage the risks associated with e-mail use and provides strategic insight into inbound and outbound traffic and associated liabilities — including spam, profanity, regulatory violations, and more.

The **ZixCorp User Awareness Program**[™] provides organizations with the tools they need to communicate e-mail security decisions and policies to employees and partners. The program provides materials to educate and motivate employees to use secure e-mail to its fullest and to explain the benefits of secure e-messaging.

Informed users are more likely to not only use their encryption software, but to enjoy it more than uninformed users. The User Awareness Program helps make understanding encryption easy and economical with co-branded Web sites, quick start guides, posters and internal policy letters, to help get the message across.

Exhibit 1
 “Legal & Regulatory Alignment with ZixCorp Proven Trust Model”

Laws & Rules	Sensitive Information Mandates	ZixCorp Services
Gramm-Leach-Bliley Act Data Protection	Protect security and confidentiality of customers’ nonpublic personal information. <ul style="list-style-type: none"> • Protect against unauthorized access to or use of information. • Assess risk and implement risk-based controls such as: <ul style="list-style-type: none"> <i>Encrypting</i> sensitive data in transit <ul style="list-style-type: none"> ➔ Control and protect access to computer-based media to avoid loss or damage. ➔ Secure media in transit or transmission to third parties. ➔ Policies should include use of encryption for transmission of sensitive information. <i>Testing</i> controls, systems and procedures. <i>Monitoring, auditing, and adjusting</i> for: <ul style="list-style-type: none"> ➔ Changes in technology. ➔ Business arrangements. ➔ Sensitivity of information. ➔ Internal and External threats. <i>Reporting</i> to Board or Executive Committee on material matters such as: <ul style="list-style-type: none"> ➔ Risk management & control decisions. ➔ Testing results. ➔ Security breaches or violations. ➔ Response actions and corrective measures. <i>Training</i> staff to understand: <ul style="list-style-type: none"> ➔ His or her security role ➔ Recognize, respond to, and report unauthorized and fraudulent attempts to obtain customer data. 	ZixVPM: <ul style="list-style-type: none"> • Provides strong encryption through public key technology to ensure only authorized access to information. • Enables corporate security policies to be set for the entire enterprise domain down to individual departments or users. • Scans all e-mail (to, from, subject, body, and attachment) against these policies to determine what is sensitive data, and tag it for encryption. • Provides automatic monitoring of secure e-mail policies against the financial lexicon for encryption of e-mails that contain personally identifiable financial information such as credit card numbers, account numbers, Social Security numbers and financial terms. • Provides the ability to determine an action(s) as part of the policies such as encrypt/don’t encrypt, block, forward, log, reply or bounce. • Assures that all authorized recipients, regardless of their e-mail solution, can receive and read encrypted messages. • Reduces the risk of human error. • Provides logging capabilities to give an organization the power to track all information being encrypted. ZixMail: <ul style="list-style-type: none"> • Provides desktop-to-desktop encryption. • Date and time-stamped certificate receipts ensure messages are opened and read only by intended recipients. • Assures that all authorized recipients, regardless of their e-mail solution, can receive and read encrypted messages.
Sarbanes-Oxley Act	<ul style="list-style-type: none"> • Secure information infrastructure. • Monitoring of IT processes and nonpublic information. • Risk assessment of internal controls, technology, & information security. • Public-disclosure & rapid reporting of material events. 	ZixAuditor: <ul style="list-style-type: none"> • Identifies e-mail risks and the effectiveness of e-communication policies for reporting purposes. • Tests existing policies and technology. • Reports detailed and objective traffic statistics and areas of vulnerability. Report includes categories such as personal financial information (as defined by GLBA), profanity, human resources, legal, IT, spam and intellectual property.
California Senate Bill 1386	<ul style="list-style-type: none"> • Disclose any breach of data security. • Monitoring and reporting systems to identify security breaches. • Encryption of personal data. 	<ul style="list-style-type: none"> • Facilitates comprehension of what sensitive data to encrypt to ensure compliance.
USA PATRIOT Act	<ul style="list-style-type: none"> • Risk-based systems and monitoring. • Verifying customer identity. • Report suspicious activity. 	
Identity Theft Act	<ul style="list-style-type: none"> • Protect personally identifiable information. • Monitor for exposure. • Rapid and comprehensive response program. • Report suspicious activity. 	ZixCorp User Awareness Program: <ul style="list-style-type: none"> • Provides tools to effectively communicate e-mail security decisions and policies to employees and partners. • Provides training guides for users and recipients. • Reminder literature helps ensure compliance.

NEXT STEP - PERFORM A COMPLIANCE SELF ASSESSMENT

It is difficult to imagine a financial institution that does not make full use of e-mail or other forms of electronic communications to contact customers, communicate among employees, or transmit nonpublic information. *For the safe use of e-mail, an institution should have encryption and other controls in place that ensure it can securely send and receive information without compromising that information.* The **Exhibit 2** Compliance Self Assessment checklist incorporates common controls used for e-mail communications that most institutions should use to protect information from unauthorized use or disclosure. If your institution cannot answer in the affirmative to each of the control methods, you may be at risk of employees sending or receiving information that does not follow policy and that puts your organization's reputation at risk.

Financial institutions that are interested in properly and adequately protecting nonpublic information can learn more about how ZixCorp can help maintain the security of information transmitted through e-mail by contacting sales@zixcorp.com or 1-866-257-4949.

Exhibit 2 - Compliance Self Assessment Checklist

Securing E-Mail and other Electronic Messaging	ZixCorp	Your Institution
Monitors employees' compliance with the security policy relating to e-mail.	✓	<input type="checkbox"/>
Incorporates encryption of outgoing and decryption of incoming e-mail messages.	✓	<input type="checkbox"/>
Uses content scanning for To, From, Subject line, message text, and attachments.	✓	<input type="checkbox"/>
Creates certified receipts for delivery assurance and time stamps.	✓	<input type="checkbox"/>
Provides alerts to security personnel in cases of unauthorized use.	✓	<input type="checkbox"/>

ABOUT THE AUTHORS

PAUL REYMANN

Paul Reymann is CEO of ReymannGroup, Inc., which has emerged as a national leader in providing knowledge, services, and software that help clients across multiple industries successfully navigate emerging regulatory, business, technology, and information security challenges.

Mr. Reymann is one of the nation's leading financial institutions regulatory experts and co-author of Section 501 of the Gramm-Leach-Bliley Act Data Protection regulation. Mr. Reymann has more than eighteen years experience in the financial services industry, including thirteen years with the Department of Treasury's Office of Thrift Supervision (OTS) in Washington D.C. There he guided the regulatory agency's Technology Risk management activities and authored several key regulatory directives and advisories on emerging risk management issues, including the industry's first regulatory directive on "Transactional Internet Banking."

E-Mail Encryption Responsibilities For Financial Institutions

Fortune 500 companies have leveraged Mr. Reymann's subject matter expertise to develop successful go-to-market strategies for information security and technology products and services within key vertical markets. He is referenced frequently in industry news and magazine articles. He is also the author of numerous articles and papers on technology risk and network and information security.

JULIE OLSEN

R. Julie Olson is a leading financial services expert with over 30 years of experience as a bank regulator. She worked for the Comptroller of the Currency (OCC) in various positions from 1974 until 2004. She began her career with the OCC as a bank examiner in Kalamazoo, Michigan and transferred to the OCC Headquarters Office in Washington D.C. in 1980. She served in many senior level positions with the OCC, including Director for Administration, Executive Assistant to the Comptroller of the Currency, Assistant Chief National Bank Examiner for Capital Markets, Acting Director for Management Services in Information Technology, and Director for Licensing. Julie also worked with the team providing oversight and guidance to the banking industry during the Year 2000 rollover as the agency's Year 2000 Coordinator. She has bachelor's and master's degrees in Economics.

ABOUT ZIXCORP

Zix Corporation (ZixCorp[®]) provides easy-to-use-and-deploy e-communication services that protect, manage, and deliver sensitive information to enterprises and consumers in healthcare, finance, insurance, and government. ZixCorp's eSecure services enable policy-driven e-mail encryption, content filtering and send-to-anyone capability while its eHealth services improve patient care, reduce costs, and improve efficiency through e-prescribing and e-lab solutions. For more information, visit www.zixcorp.com.

ABOUT REYMANNGROUP, INC.

ReymannGroup, Inc. provides finance, healthcare, retail and manufacturing 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 books, and subject matter experts familiar with financial, healthcare, retail and manufacturing 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. Learn more by visiting www.reymanngroup.com.