

# The Case for Email Encryption

## Required by Law

Securing the personal information of customers, partners and employees is more than just a value-added service—it's often the law. Compliance is closely monitored by a number of government and regulatory bodies.

Here's a quick look at some of key links pertaining to email encryption and its examination by regulatory bodies:

**The Gramm-Leach-Bliley Act (GLBA)** of 1999 protects consumers' personal financial information held by financial institutions. Its "Safeguards Rule" requires all financial institutions to design, implement and maintain safeguards to secure confidential data.

Its guidelines address standards for developing and implementing administrative, technical, and physical processes to protect the security, confidentiality, and integrity of customer information. For more information, click on:

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

In GLBA's Section 501(b), the **Federal Deposit Insurance Corporation (FDIC)**, the **Board of Governors of the Federal Reserve System**, the **Office of the Comptroller of the Currency**, and the **Office of Thrift Supervision** have been ordered to establish standards for protecting the security and confidentiality of financial institution customers' non-public personal information. This came into effect on July 1, 2001. To learn more, go to:

<http://www.fdic.gov/news/news/financial/2001/fil0168.html>

Under the GLBA's examination of procedures to evaluate, the encryption of electronically transmitted and stored customer data is listed as a key area to manage and control an institution's risk:

<http://www.fdic.gov/news/news/financial/2001/fil0168a.html>

## ZixDirectory Includes

- Over 15 million protected email addresses and growing at 100,000 new recipients every week
- The FFIEC federal banking regulators and the Securities and Exchange Commission
- Over 20 state bank regulators
- More than 800 financial institutions
- 3 out of the 5 largest US health insurance companies
- More than 1,000 hospitals in the US (1 in every 7)
- Over 30 Blue Cross Blue Shield Institutions

## News Alerts:

- ZixCorp's ZixVPM 3.3 voted *Network Products Guide's* 2008 Reader Trust Award Winner for Best in Secure Email
- Positioned in the Leader's Quadrant in Gartner's *Magic Quadrant for Email Encryption*

In 2006, The **Federal Financial Institutions Examination Council (FFIEC)** released a handbook on information security practices. Regarding encryption, it stated that financial institutions should use encryption to mitigate the use of disclosure or alteration of sensitive information in storage and transit. Encryption should include:

- Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk
- Effective key management practices
- Robust reliability
- Appropriate protection of the encrypted communication's endpoints

For more information, visit:

[http://www.ffiec.gov/ffiecinfobase/booklets/information\\_security/information\\_security.pdf](http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf)

**The Federal Deposit Insurance Corporation (FDIC)** released an information technology questionnaire that underscores the GLBA's Section 501(b) on data security. It is aimed at Information Technology Officers (CTOs) of financial institutions with questions on their banks' IT operations, governance programs and information security, with specific reference to their encryption practices surrounding customer information:

<http://www.fdic.gov/news/news/financial/2007/fil07105a.pdf> and  
<http://www.fdic.gov/news/news/financial/2007/fil07105.html>

**The State of Nevada** passed a law in October 2008 that all businesses, no matter how small they are or what they do, must secure confidential customer information if it is sent electronically. Statute 597.970 states that any form of Internet communication, including via web sites and email, must encrypt personal data:

<http://www.leg.state.nv.us/Nrs/NRS-597.html#NRS597Sec970> and  
<http://online.wsj.com/article/SB122411532152538495.html>

**The Commonwealth of Massachusetts** has mandated that, effective January 1, 2010, companies are required to encrypt all personal information of state residents transmitted electronically or wirelessly. This includes Social Security and employer-identification numbers, drivers' license or identity card data, account, credit and debit card numbers with any password or security and access codes. For more background, click on:

[http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090212\\_idtheft&csid=Eoca](http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090212_idtheft&csid=Eoca)

## ABOUT ZIXCORP

ZixCorp provides easy-to-use-and-deploy email encryption and e-prescribing services that protect, manage and deliver sensitive information to the healthcare, finance, insurance and government industries. ZixCorp's hosted Email Encryption Service enables policy-driven email security, content filtering and send-to-anyone capability. Its PocketScript e-prescribing service provides point-of-care access and transmission of patient and payor data that improves patient care, reduces costs and improves efficiency.

For more information about ZixCorp call toll free **866-257-4949**, email [sales@zixcorp.com](mailto:sales@zixcorp.com) or visit [www.zixcorp.com](http://www.zixcorp.com).