The Gramm-Leach-Bliley Act (GLBA) secure messaging white paper

Introduction

The Gramm-Leach-Bliley Act (GLBA), enacted in 1999, provides a number of provisions to protect consumers' private financial information against exploitation and loss while in the hands of financial institutions and other organizations. As financial institutions have evolved since 1999, the way they maintain, use and transmit customer information has dramatically shifted with the adoption of electronic communications, namely email. Now transactions move faster and business processes are streamlined. Yet, despite the expediency of digital age communication, email poses a new challenge to securing customer financial data against loss or unauthorized exposure. Email remains vulnerable to:

- **Malware:** Commonly downloaded through infected email attachments and executable files, viruses and other malware can infect a messaging system to delete files, damage programs, access and capture sensitive data for exploitation.
- **Phishing:** Fraudulent emails appearing as authentic and legitimate attempt, and often succeed at getting unsuspecting users to give up sensitive data for financial exploitation.
- **User-error:** When it comes to data leakage, users are leading cause. According to a 2011 study by the Ponemon institute, 69 percent of organizations surveyed indicated employees violated security policies frequently and send confidential and sensitive information via non-approved, unsecured email methods.

While email remains vulnerable, customer information exchanged through the email gateway remains susceptible to unauthorized exposure and loss. Tasked with securing customers' private information under GLBA, email's vulnerabilities underscore the need for financial institutions to secure email communications to ensure the security and integrity of customer information exchanged via email.
This white paper briefly details how GLBA affects email security for financial institutions, and what technologies financial services providers can implement to help ensure secure, GLBA-compliant email communication and file transfer.

Who is affected by GLBA?

GLBA broadly applies to organizations within the financial industry. These include financial institutions in the traditional sense such as banks, credit unions and mortgage lenders as well as additional businesses that provide products and services of a financial nature. Such services include but are not limited to:

- Investment Advisory Services.
- Tax Planning & Preparation.
- Insurance Sales and Underwriting.
- Check cashing, Money Transfers and Money Orders.
- Consumer Lending or Leasing.
- Credit Card Activities.

Businesses that provide financial products and services like those above, by nature, utilize a broad range of customers' nonpublic personal information (NPI)--credit card numbers, bank account information, social security numbers - data that GLBA seeks to protect against damage or exploitation. As a result, GLBA charges affected businesses to protect nonpublic customer information or face biting civil and criminal penalties.

Why should my organization comply with GLBA?

To compel financial services providers to comply with requirements, GLBA imposes biting financial and criminal penalties on businesses and executives that fail to protect NPI using prescribed safeguards. For each violation, a financial institution can be fined up to $100,000 while its executives can be fined up to $10,000 and face imprisonment for up to 5 years. Additionally, if GLBA is violated at the same time that another federal law is violated, or if GLBA is violated as part of what the SEC deems a pattern of compliance violations within a 12-month period, the violator's fine will be doubled and he or she can imprisoned for up to 10 years.

What does GLBA require for email compliance?

The act places responsibility on financial institutions to protect customer financial data and personal identifying information, which it calls nonpublic personal information (NPI), in their possession wherever it resides--including email. Specifically two key components of the act directly impact email security: the Safeguards Rule and a provision for ***Pretexting Protection*.**

The Safeguards Rule requires that affected institutions **(1)** conduct a thorough risk assessment of its security measures and **(2)** "develop, implement, and maintain a written information security program" that contains administrative, technical, and physical safeguards to:

1. Ensure the security and confidentiality of customer records and confidential information when stored and transmitted.
2. Proactively protect against any anticipated threats or hazards to the security or integrity of these records.
3. Protect against unauthorized access to or use of records that could cause customers to sustain substantial harm or inconvenience.

GLBA mandates that additional safeguards be implemented to address what it calls ***Pretexting***, or fraudulent attempts to access and exploit customer NPI. Exploits of this nature include phishing scams, social engineering, email spoofs or other attempts to impersonate a customer by obtaining NPI.

How can my organization meet these requirements?

GLBA does not explicitly identify specific policies and email technologies organizations should implement as safeguards to achieve compliance; every institution is unique and uses NPI in different forms, for different reasons. Yet, several technologies and policy-best practices stand out as clear solutions to meet GLBA requirements in relation to email:

- **End-to-end encryption:** To meet regulation requirements that mandate NPI be secured, an end-to-end encryption that can encrypt or block content is often necessary to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss.

- **Data Leak Prevention (DLP):** A DLP solution for email is essential for GLBA compliance, providing enhanced mail security through content filtering, authentication, and permissions rules that limit access and transmission of sensitive information sent within and outside the organization.
- **Archiving.** An effective email archiving system will enable organizations to meet control objectives for message retention and auditing by capturing, preserving and making all email traffic easily searchable for compliance auditors to evaluate. When encrypted and backed-up, archiving provides additional protections for information against loss and unauthorized exposure.
- **Anti-Spam & Anti-Virus:** Protections from spam, phishing, and malware such as email filters and antivirus software will also demonstrate adequate protections against unanticipated threats to the integrity and security of NPI.
- **User Training & Awareness:** While the right mix of email security technologies is necessary to achieve compliance, technologies are only as smart as the people using them. Educate users on acceptable use policies for email; train them to identify fraudulent email, phishing scams and other *pretexting* that threatens the security of messaging system and integrity of customer information floating within it.

Don’t sacrifice functionality for compliance

While it is important to implement a solution for secure email that conforms to GLBA requirements, often technologies created to ensure regulatory compliance inhibit email functionality and workflow, frustrating users and inhibiting productivity. According to a 2011 study by the Ponemon Institute, over half of email encryption users were frustrated with their encryption solutions being inflexible and difficult to use. Email security should complement existing email rather than complicate it. So when considering a solution for secure email, it’s important that it conforms to GLBA requirements without compromising the functionality and workflow of existing email that your business depends on. This means implementing a solution that allows easy and scalable deployment, simplifies management complexity, and works with your existing email infrastructure to enable user-productivity and email functionality.

The Secure Messaging Platform is a cloud solution for email encryption, secure file transfer and DLP that helps address GLBA technical security safeguard standards, and lets you use your email just the way it is.

The Secure Messaging Platform:

- Simplifies the complexity of secure communication and collaboration, preserving workflow by integrating seamlessly with any email platform including MS Outlook, MS Office 365, Gmail and Zimbra (for both sender and recipients regardless of their network configuration).
- Conforms to GLBA technical requirements for secure transmission of NPI.
- Safeguards confidential emails and files from unauthorized disclosure or loss through powerful DLP tracking features and permissions tools; additionally allowing recall of messages and attachments even if the content has already been read.
- Automates and securely delivers messages and file attachments decrypted to any email archive database or third party application through a secure API.
- Enables anytime, anywhere secure communication and collaboration by allowing users to send, track and receive secure email and attachments on any mobile device including iPhone, iPad, Android, BlackBerry and Windows Phone.

The Secure Messaging Platform offers the most flexible solution to help address GLBA technical security safeguard standards for email and file transfer.

About the secure messaging platform

The makers of the Secure Messaging Platform believe that email security should complement your email, not complicate it. Our cloud-based solutions for secure file transfer and email encryption work seamlessly with any email to enable secure communication and collaboration anytime, anywhere.