

# Compliance Brief: GLBA



## Protect Customers' Financial Information

*The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLBA, opened competition among financial institutions, including banks, securities companies and insurance providers. It allows commercial and investment banks to consolidate and includes provisions that govern the collection, disclosure and protection of consumers' nonpublic or personally identifiable information.*

### Applicability

GLBA compliance is mandatory not only for all financial companies, including those that provide financial products and services to consumers, but for their vendors as well. Regardless of whether they disclose nonpublic information, companies must adhere to the GLBA and have policies in place to protect information. Eight federal agencies and state authorities enforce the GLBA, and penalties for noncompliance may result in up to 10 years in prison and \$1 million in fines.

### Financial Services Industry Impact

Under the GLBA, financial companies must follow three principals to safeguard information from threats to security. The Financial Privacy Rule states companies must provide each customer with a copy of privacy practices. The Safeguards Rule requires a written information security policy, and the Pre-Texting Protection Rule requires that information be protected from unauthorized access. Thus, the GLBA requires financial companies to research and implement:

- Efficient means for information distribution.
- Proven security procedures to protect personal information.
- Proactive measures to prevent and guard against threats to security and integrity.

*“As part of its implementation of the GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions to have measures in place to keep customer information secure. But safeguarding customer information isn't just the law. It also makes good business sense. When you show customers you care about the security of their personal information, you increase their confidence in your company.”*

- FTC Facts for Business, Financial Institutions and Customer Information: Complying with the Safeguards Rule

### ECM Enables GLBA Compliance

Enterprise Content Management (ECM) provides document controls and system securities that enable unified compliance and operational efficiency. Many financial companies, banks and insurance agencies use Digitech Systems' ECM solutions to address GLBA privacy and security regulations. Whether companies store information on-premise with PaperVision® Enterprise, or they outsource data storage and access information online through ImageSilo®, they can improve productivity and reduce content management costs while maintaining a compliant environment.

*PaperVision Enterprise and ImageSilo capabilities enable financial institutions to fulfill GLBA requirements and protect customer information.*

### Efficient Information Distribution

Under the Financial Privacy Rule, companies must supply each customer with a privacy notice that explains what customer information is collected and how it is shared, used and protected. ImageSilo and PaperVision Enterprise simplify document distribution and provide a secure means for sharing policies.

- Document disclosure enables financial companies to share an unlimited number of privacy notices with customers.
- Document grants allow secure, temporary, web-based access to documents for customers who prefer to receive information electronically.
- Enhanced auditing logs every customer notice sent and provides a report indicating who received the information, when and how.

### Security to Protect Customer Information

The Safeguards Rule requires companies to review how they manage personal information and analyze their systems and policies. A written information security plan must describe how the company maintains customer confidentiality. Digitech Systems' ECM solutions provide extensive security measures that help ensure administrative, technical and physical safeguards of all customer data.

- Application security includes user passwords and flexible user rights that limit physical access, and enable companies to maintain tight control over system use.
- Document security restricts employee access to personal information and ensures that staff members view only documents they need to perform their job functions.
- 256-bit AES encryption can occur both during transmission and when stored, so private financial information is protected at every step.

### Safeguards that Defend Against Threats to Security

GLBA provisions require financial institutions to protect information from unauthorized access—even when someone uses phishing methods, deception or scams to manipulate companies into divulging confidential information. PaperVision Enterprise and ImageSilo provide tools to proactively guard against malicious attacks.

- Security access rights are verified for every information request submitted to the ECM system.
- Enhanced auditing tracks all user activity, including successfully completed, attempted or suspicious activities, such as trying to open protected records without security clearance.
- ImageSilo employs a third party to scan the network, verify immunity to the latest exploits and validate security on a daily basis.