

Document Management Solutions for Gramm-Leach Bliley- Safeguards Rule Compliance

Companies are establishing compliance management measures to proactively manage their organizational risk. The task of managing compliance for an organization has become a challenging endeavor with the increasing costs of compliance failure, - fines, litigation, and criminal penalties. Companies are searching for solutions that provide them with a way to manage this growing challenge.

To achieve regulatory compliance, financial service organizations need to apply technology to secure access of data, to ensure the physical protection of data and to create an audit trail showing who has had access to the data. Document Imaging is a key solution for helping financial service organizations achieve these technological objectives.

Many financial institutions collect personal information from their customers, including names, addresses, and phone numbers; account numbers; income and credit histories; and Social Security numbers. The **Gramm-Leach-Bliley (GLB) Act** requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of personal information. The GLB Act impacts banks, insurance companies, mortgage companies, securities brokers, loan brokers, some financial or investment advisors, tax preparers, providers of real estate settlement services and debt collectors.

GLB defines security guidelines for bank and financial service organizations regarding privacy of customer information. GLB had a number of specific security objectives including:

- Ensure security and confidentiality of customer information.
- Protect against anticipated threats or hazards to security or integrity of information.
- Protect against unauthorized access to or use of the customer information.

As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information safe and secure. But safeguarding customer information is not just the law; it also makes good business sense.



HOW TO COMPLY

The Safeguards Rule requires companies to develop a written security plan describing their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- **Designate** one or more employees to coordinate its information security program;
- **Identify and assess** the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- **Design and implement** a safeguards program, and regularly monitor and test it;
- **Select service providers** that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- **Evaluate and adjust** the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

SECURING INFORMATION

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures. One of the early steps companies should take is to determine what information they are collecting and storing, and whether they have a business need to do so. You can reduce the risks to customer information if you know what you have and keep only what you need.

The following table contains items that are required for Safeguards Rule compliance and how by implementing a document management solution, businesses can meet the requirements:



Requirement	Document Management Implementation
<p>Access Control: Limiting access to customer information to employees who have a business reason to see it.</p> <p>For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.</p>	<p>User-Based Access- document management solution should include a mechanism for establishing and modifying user access to documents.</p> <p>Access management tools allow managers the ability to determine the extent of an individual's access to any file while protecting confidential documents from unauthorized viewing or tampering.</p>
<p>Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis.</p>	<p>Password Protection- Document management solution should include a password authentication mechanism.</p>
<p>Entity Authentication: Using password-activated screen savers to lock employee computers after a period of inactivity.</p>	<p>Password Protection- Document management solution should include a password authentication mechanism.</p> <p>Automatic Logoff- should have a mechanism for automatically logging off users that have been idle for too long.</p>
<p>Contingency Plan: Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.</p>	<p>Data Backup Plan - document management solution should have a mechanism for backup of database and all image files for safe offsite storage.</p> <p>Disaster Recovery- solution should have the ability to rebuild its database from archived files in the event of serious database failure.</p>
<p>Take steps to ensure transmission of customer information.</p>	<p>Data Authentication- document management solution should include a mechanism to ensure that documents have not been tampered with.</p>

<p>Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.</p>	<p>Audit Controls- document management should include mechanisms for auditing all types of document access. Auditing capabilities should include modifications to user rights, logons, logoffs, and failed logon attempts.</p> <p>Additional audit procedures include an Audit Trail feature. Audit Trail automatically keeps track of every time someone creates, annotates, prints, views or deletes documents. Audit Trail also informs managers when a document or file was accessed, what was done and who did it.</p>
<p>Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information</p>	<p>Audit Controls- document management should include mechanisms for auditing all types of document access with Audit Trail.</p>

The complete Rule is available at www.ftc.gov/privacy/privacyinitiatives/safeguards_lr.html

Please see FTC Facts for Business- Financial Institutions and Customer Information: Complying with the Safeguards Rule <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.pdf> for complete details. <http://www.ftc.gov/>

Federal Trade Commission -16 CFR Part 314-Standards for Safeguarding Customer Information; Final Rule <http://www.ftc.gov/os/2002/05/67fr36585.pdf>

For more information on e-mail compliance or to see how PiF Technologies fulfills these requirements, please call 888-934-4443.



Disclaimer

This document is provided by docSTAR to our partners and customers in an attempt to answer some of the questions of The Gramm-Leach-Bliley (GLB) Act. The information provided herein is only intended to be a general summary of the subject matter. While every effort has been made to provide accurate information, no guaranty or warranty, express or implied, is made about the accuracy, currency, completeness or adequacy of the information provided, and no liability is assumed for any errors or omissions with respect to that information. The information is intended for educational purposes only and is not legal advice and should not be used as a substitute for legal or other professional advice. Each person and/or business should consult with counsel, as appropriate, concerning the applicability of this information to the particulars of their situation.

