



GRAMM LEACH BLILEY ACT

**SOURCECOPY**<sup>SM</sup>

Powered By: **Asigra.**

[www.site2bc.com](http://www.site2bc.com)



# GRAMM LEACH BLILEY & SOURCECOPY

## Executive Summary

GLBA repealed the Glass Steagall Act permitting banks to, once again, offer investments, commercial banking and insurance products. Included in the act are compliance components that govern the collection and disclosure of a customers' personal financial information. The Financial Privacy Rule governs how financial institutions collect and disclose a customers' personal financial information. It also applies to companies other than financial institutions who receive such information. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information.

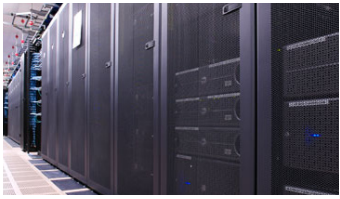
## Safeguards Rule

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule also applies to information of those who are no longer consumers of the financial institution.) This plan must include:

- >> Denoting at least one employee to manage the safeguards,
- >> Constructing a thorough [risk management] plan on each department handling the nonpublic information,
- >> Develop, monitor, and test a program to secure the information, and Change the safeguards as needed with the changes in how information is collected, stored, and used.

The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions. GLBA compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

This rule is intended to do what most businesses should already be doing: protect their clients. The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial institution has had to make some effort to comply with the GLBA.



## **Financial Privacy Rule**

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt-out of the information being shared with unaffiliated parties per the Fair Credit Reporting Act. Should the privacy policy change at any point in time, the consumer must be notified again for acceptance. Each time the privacy notice is reestablished, the consumer has the right to opt-out again. The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement. In summary, the financial privacy rule provides for a privacy policy agreement between the company and the consumer pertaining to the protection of the consumer's personal nonpublic information.

## **Enforcement**

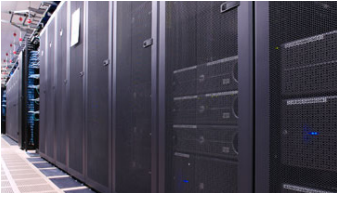
### **Industry Enforcement**

Service organizations providing services to companies in the financial services industry (ex. Insurers) are being required to have a SAS 70 review conducted to comply with GLBA requirements. SAS 70 is an auditing statement and the professional standards used by an auditor to assess the internal controls of a service organization. Service organizations that provide services to healthcare companies are asked by their clients to have a SAS 70 audit conducted to ensure a third party has examined the controls over the processing of healthcare information due to its sensitivity.

### **Legal Enforcement**

Violation of the GLBA may result in a civil action brought by the United States Attorney General. The penalties, as amended under the Financial Institution Privacy Protection Act of 2003 include,

1. "The financial institution shall be subject to a civil penalty of not more than \$100,000 for each such violation"
2. "The officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation".



More than 25 states have passed data privacy or breach notification laws that require organizations to notify consumers when their information may have been exposed. One high profile example is California SB1386. This statute went into effect July 1, 2003, under California Civil Code Section 1798.29, and requires notification to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

### **SourceCopy Applicability**

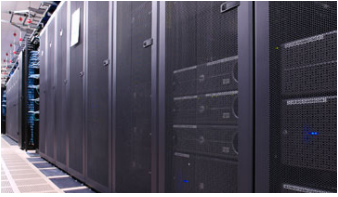
**Risk Mitigation** – Financial firms, including insurers, are very risk conscious. To mitigate their risks and to comply with regulation such as GLBA, they implement policies and controls. An example policy is a company's business continuity and disaster recovery plan. The implementation of such a plan includes procedures and controls that can help a company achieve resiliency. However, in the process, the plan must not jeopardize GLBA.

A common disaster recovery solution is computer data backup using tape media. While tapes can help the company achieve its disaster recovery goals, they can also create gaps in the company's GLBA compliance efforts.

**Security and Privacy** – The SourceCopy online backup solution can help a financial institution achieve disaster recovery goals while also complying with GLBA. This is accomplished by providing a secure, private and automated system for protecting client records from virtual and physical disasters while also offering the following security and privacy controls:

**User authentication** – SourceCopy requires system users to identify themselves using a user id and password. This is unlike many traditional backup solutions including tape. As a medium, tape cannot restrict a user's ability to access confidential stored information once they gain physical access to it. Achieving access to data on tape is as simple as placing the tape into an appropriate tape drive.

**Role based authorization** – Once authenticated to the SourceCopy system, each user is restricted, by granted permission levels, to the type of information they can and cannot backup and restore. For example, someone in the accounting department may not be able to access human resources information. These restriction levels should be in line with authorization controls on the company's network and computer systems.



**Data Compression and Encryption** – these two technologies make unauthorized data access virtually impossible and are core to the SourceCopy offering. The client’s information is stored using compression (reducing the file size) and encryption (making the information unreadable) so that the data cannot be ‘read’ while in transit (i.e. transmitted from the client location to the SourceCopy storage facility) or at rest (i.e. while maintained in the storage system). By contrast, tape based solutions typically store their information in clear text, therefore allowing someone who gains access to the tape, either in transit or at rest, to understand its contents . Tape solutions can add encryption technology, but this approach typically requires additional software licensing (i.e. additional expenses) and additional manual procedures.

**Secure offsite data storage** – disaster recovery backup solutions must afford the same level of security and privacy to the backed up data as what is afforded in the source computer system. When information is moved to a tape, it is no longer on the computer system that once protected it. The company is no longer affording the same security level to their data. SourceCopy protects the client’s data at all times, therefore helping the client afford the appropriate level of security and privacy to their backup solution.

**Audit logs/trails** – controls and procedures are required to ensure security and privacy. An often sought after control by auditors is audit trails which log all activity associated with the backup processing and overall administration and maintenance of the system. SourceCopy provides detail trails identifying who, what and when activities were performed.

### ROI

In addition to these security and privacy controls, SourceCopy offers a robust disaster recovery solution without the capital expense of traditional backup solutions that typically require hardware and software investments. SourceCopy can be classified as an operational expense since the client effectively “rents” the amount of backup storage required to meet their needs – no investment in hardware or software. Traditional software backup solutions require the client to purchase client agent software for every computer that they are going to protect. Additional fees are typically charge for multiple operating systems need protection as well as different types of software applications needing protection. SourceCopy does not charge by the computer being protected. The SourceCopy software is free and can be installed on as many client computers as is required. SourceCopy is priced based on the amount of storage the client uses in our computer vault. Over a 3 year contract, this is typically far less that the licensing required by traditional backup software.

The SourceCopy solution can also eliminate additional fees associated with purchasing new/ replacement tapes, upgrading tape drives, maintaining the tape drive, FTE’s associated with backup operations and offsite tape custodial/storage solutions.

**For More Information:** [http://en.wikipedia.org/wiki/Gramm-Leach-Bliley\\_Act](http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act)

Proprietary & Confidential © 2009 Site2, LLC.