



Mirrored Storage, Inc.

Data Backup and Compliance Legislation - GLBA

White Paper presented by:

Mirrored Storage, Inc.

ONLINE BACKUP SOFTWARE

<http://MirroredStorage.com>

Introduction

The amount of data used by today's businesses has increased exponentially from just five years ago. Corporate scandal, international unrest, and glaring security flaws in computer operating systems and software applications have resulted in a much more intense and detailed analysis of data as it enters and leaves the enterprise. Fortune 500 companies have been vilified in the press for reckless data stewardship, and in some cases of outright fabrication of financial and performance reports. In extreme cases, executives are now lounging in Federal facilities, denying to the bitter end that they had any knowledge of the blatant misrepresentation for which they were held accountable.

The private information stores of several prestigious organizations, some of them very sensitive and personal in nature, have been lost, misplaced, or accessed by hackers – the details of the events becoming fodder for an indignant news media.

Corporate America, already under varying degrees of competitive and performance pressure, is now faced with compliance legislation and disclosure requirements that seek to right some of the wrongs done to consumers, investors, and employees alike. What follows is an analysis of the major pieces of process and data management compliance legislation, with a specific focus on the critical role that data availability plays in all of them. Access and process controls, internal and third party audits, reporting requirements and penalties for non-compliance are just a few of the areas that will be addressed on a per-measure basis.

The Financial Modernization Act of 1999 - Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB, includes provisions to protect consumers' personal financial information held by financial

institutions. There are two principal parts to the privacy requirements as they relate to data management: the Financial Privacy Rule and the Safeguards Rule.

The GLB Act gives authority to eight federal agencies and the States to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These regulations apply to “financial institutions,” which include not only banks, securities firms, and insurance companies, but also companies providing many other types of non-traditional financial products and services to consumers. Among these services are those in the business of lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, residential real estate settlement services, collecting consumer debts, providing health insurance and an array of other activities. Such non-traditional financial institutions are also regulated by the FTC¹.

The Financial Privacy Rule governs the collection and disclosure of customers’ personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information. The Financial Privacy rule requires covered institutions to spell out, in the form of a privacy notice, their information sharing practices. Most of us have seen these notices included with correspondence related to loan applications, account servicing, or credit card statements. Using a process detailed in the institutional privacy notices, consumers have the right to limit some – but not all – sharing of their information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The rule applies not only to financial institutions that collect information from their own customers, but also to businesses – such as credit reporting agencies – that receive customer information from those institutions. It is within the Safeguards section of GLB that the parameters for data safety at these institutions are clarified, and it is here also that the deficiencies of ‘legacy’ data protection methods are exposed. The section addresses distinct areas of safeguards which must be implemented, including Administrative, Technical, and Physical.

As in HIPAA regulations, many of the Administrative safeguards are designed to verify that reasonable steps are being taken to secure the sensitive data stores maintained by covered institutions. While most of these steps should be (and in many cases are already) taking place at the institutions, the Safeguards Rule mandates that the administrative steps be encapsulated in a written information security plan. The plan is required to include an assessment of risks and an evaluation of existing safeguards, the establishment of a comprehensive safeguards plan, contracting with vendors to facilitate the plan when appropriate, and regular testing and evaluation of the plan and practices as the covered entity’s business scope or volume changes.

The Federal Trade Commission (FTC), which is a major oversight body for GLB, also indicates the need for employee education and training, information systems management, and managing system failures. These measures help to insure that data safeguards are robust and that all parties who come into contact with sensitive information are aware of company policies and the law.

The Information Systems component of GLB addresses the company’s technological interfaces with client data, and can include analyses of network and software design, information processing, storage, transmission, retrieval, and disposal. Here again, The FTC strongly

suggests several procedural and technological steps ranging from basic security like locked file drawers and server rooms to backing up client data to a secure, encrypted and password-protected server.

Many of GLB's provisions are designed to ensure that basic steps are taken to ensure client data is only available to those employees who need it in the course of their work, and that it is securely off-limits to others. The Financial Privacy provisions were put in place to insure that the data is properly maintained and protected. The provisions related to information systems and managing systems failures help to insure that the institution maintains access to the data in order to resume operations after data loss, and to be able to provide documentation that would normally have been lost when and if the need or requirement arises.

As Federal agencies are empowered to enforce GLB under existing codes such as the Federal Deposit Insurance Act, penalties for non-compliance are substantial. Fines levied at guilty institutions can be up to \$100,000 per violation at the national level and can also expose the covered institutions, especially those in the insurance sector, to state-level sanctions in many cases. In addition, the officers and directors of these companies can be held personally liable for civil penalties up to \$10,000. For companies or individuals that employ 'pretexting' (the use of fraudulent or deceptive tactics to obtain private financial information) the monetary penalties can go even higher, and violators can face prison terms of 5 to 10 years in addition to the fines.

Data Backup Software and Services – Access controlled Data Insurance

To be clear, there is no single software product or information technology service that can make an organization fully compliant with any of this legislation. The respective laws are complex and far-reaching, and were designed to enforce a level of integrity in operations and corporate philosophy that cannot be pulled from a box or jewel case. Remote Backup Software, through its ability to maintain secure copies of critical, sensitive data in a protected location, and to have them available for quick restore for required reporting or disclosure, addresses several of the criteria of compliance with all of them.

As enforcement of these laws increases, so does the need to have your data, and that of your clients, properly secured. Are you a member of the 'circle of trust' as referenced in GLB? Are you a HIPAA 'covered entity' or a business partner of one? Can you guarantee availability of critical reporting data for your SOX clients? It is time for IT service companies and businesses of all types to get serious about data security – and remote backup of data is a crucial and cost-effective component in compliance, business continuity, and disaster recovery planning.

Acknowledgements and Sources:

1Federal Trade Commission, Financial Privacy: The Gramm-Leach Bliley Act, online at ftc.gov

Media Contact information:
John Neibel, President & Founder
[Mirrored Storage, Inc.](http://MirroredStorage.com)
P. 214-550-0550



Copyright © 2010, [Mirrored Storage, Inc.](http://MirroredStorage.com) Any reuse without the expressed written permission of [Mirrored Storage, Inc.](http://MirroredStorage.com) is prohibited.