



“The Mortgage Specialists”

Gramm-Leach-Bliley Act

THE MONEY SOURCE, INC.

IT –Security and Policy

May 12, 2010



591 Stewart Avenue, Suite 100
Garden City, NY 11530

Tel: (516) 542-8500 / Fax: (516) 542-8530

Licensed Mortgage Lender, FNMA Approved Seller Servicer, Ginnie Mae Approved Issuer

OBJECTIVES FOR GLBA

- What is GLBA?
- Why does it apply to The Money Source, Inc.?
- How does The Money Source, Inc. comply with GLBA
- What is the penalty if The Money Source, Inc. does not comply
- GLBA Terms and Definitions

What is GLBA?

- The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting financial institutions. The law requires financial institutions to develop, implement and maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of customer information.
- The GLBA is composed of several parts, including the Privacy Rule(16 CFR 313) and the Safeguards Rule(16CFR314)

Why does the GLBA Safeguards Rule apply to The Money Source, Inc.?

- The Money Source, Inc. engages in the origination, processing, underwriting and closing of mortgage loan applications, and as a Mortgage Lender, falls under the definition of “Financial Institution” under the GLBA and must comply with the laws and requirements.
- “Financial Institution” means any institution, the business of which is engaging in financial activities.

Examples of Financial Activities That Are Covered by GLBA:

- Obtaining information from a consumer report
- Financial or investment advisory services
- Credit counseling services
- Receiving loan application information and the making and servicing of such loans
- Collection of delinquent loans
- Career counseling services for those seeking employment in finance, accounting or auditing
- Check cashing services
- Tax planning and tax preparation

GLBA Definitions

- Customer information is any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates

Non-Public Personal Information means personally identifiable financial information that is:

1. Provided by a consumer to a financial institution
2. Resulting from any transaction with the consumer or any service performed for the consumer; or
3. Otherwise obtained by the financial institution

The term also includes any list, description or other group of consumers and publicly available information pertaining to them that is derived using any personally identifiable financial information that is not publicly available.

Examples of Nonpublic Personal Information (NPI) Include:

- Social security Number (SSN)
- Financial account numbers
- Credit Card numbers
- Date of birth
- Name, address, and phone numbers when collected with Financial data
- Details of any financial transactions

GLBA Safeguards Rule

- The Safeguards Rule requires all financial institutions to develop an information security program designed to protect “customer information.”
- “Information Security Program” means the administrative, technical or physical safeguards used by a financial institution to access, collect, distribute, process, protect, store, use, transmit, dispose of or otherwise handle customer information.
- In addition to developing their own safeguards, financial institutions are responsible for taking steps to insure that their affiliates and service providers safeguard the customer information in their care.
- “*Affiliate*” means any company that controls, is controlled by or is under common control with another company.
- “Service Provider” means any person or entity that receives, maintains, processes, or otherwise is permitted to access customer information through its provision of services directly to a financial institution.

Safeguards Rule Objectives

The objectives of the GLBA Safeguards Rule are to:

1. Insure the confidentiality and security of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of this information and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Safeguard Rule requires financial institutions to develop an information security program that includes the following:

1. Designate a Security Program Coordinator responsible for coordinating the program-The Money Source, Inc. Compliance Officer is hereby designated
2. Conduct a risk assessment to identify reasonably foreseeable security and privacy risks
3. Ensure that safeguards are employed to control the identified risks and regularly test and monitor the effectiveness of these safeguards
4. Oversee service providers, including selection of appropriate service providers and use of contract language to protect customer information handled by service providers and
5. Evaluate and adjust the information security program in light of relevant circumstances and changes in the business

Information Security Safeguards

When The Money Source, Inc. implements safeguards to protect the security, confidentiality, and integrity of customer information, there are three types of safeguards to consider:

1. Administrative Safeguards
2. Technical Safeguards
3. Physical Safeguards

Administrative safeguards include:

- Checking references on potential employees
- Training employees to take basic steps to properly protect customer information.
- Limiting access to customer information to only those employees who have a business need to see such information
- Asking every new employee to sign an agreement to follow the confidentiality and security standards for handling customer information.
- Instructing and regularly reminding all employees of the legal requirement and of University and departmental policy to keep customer information secure and confidential.
- Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.
- Imposing disciplinary measures for any breaches in policy
- Referring all requests for customer information to designated individuals who have had safeguards training.
- Recognizing fraudulent attempts to obtain customer information and report to law enforcement agencies.

Physical safeguards include:

- Storing paper records in a locked room, cabinet or other container
- Using password activated screensavers
- Using strong passwords(at least 8 characters long)
- Changing passwords periodically and not sharing passwords or writing them down
- Ensuring that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods
- Disposing of customer information appropriately

Technical Safeguards include:

- Storing electronic customer information on a secure server that is accessible only with a password or has other security protections and is kept in a physically secure area.
- Maintaining secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.
- Avoiding storage of customer information on machines with an internet connection.
- Encrypting sensitive customer information when it is transmitted electronically over networks or stored online.
- Maintaining up to date firewalls
- Using anti virus software that updates automatically
- Obtaining and installing software patches promptly
- Following written contingency plans to address breaches of safeguards

Guidelines for Providing Secure Data Transmission

- When collecting information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail.
- If you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.

Guidelines for Secure Disposal of Customer Information:

- Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up
- Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information.
- Promptly dispose of outdated customer information.

Managing System Failures

- Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures.
- Effective security management requires policies and procedures to deal with these failures

Maintaining Up to Date Programs and Controls

- Follow a written contingency plan to address any breaches of physical, administrative or technical safeguards
- Check with software vendors to regularly obtain and install patches that resolve software vulnerabilities
- Use anti-virus software that updates automatically
- Maintain up to date firewalls particularly if using broadband internet access or allowing employees to connect from home or other off site locations.
- Provide central management of security tools for employees and pass along updates about any security risks or breaches.
- Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. Back up all customer data regularly.
- Maintain systems and procedures to ensure that access to non public consumer information is granted only to legitimate and valid users.

- Notify customers promptly if their non public personal information is subject to loss, damage or unauthorized access.

Role of IT Security & Policy in GLBA compliance

- Risk assessments
- Guidelines for secure computer data
- Educational Materials
- Providing security tools and software
- Providing support for security issues
- Security event response

Enforcement of the GLBA

- The FTC may bring an administrative enforcement action against any financial institution for non compliance with the Safeguards Rules.
- Penalties for violating SafeGuards Rule would likely include equitable damages caused by the loss of privacy, for example, a breach of security resulting in identity theft.