

# Customer Privacy – Preventing Privacy Breaches

MBA's Document Custody Conference  
September 9-11, 2007  
San Antonio, TX

**Paul H. Schieber**

**Diane Slifer**

**Blank Rome LLP**

**(215) 569-5500**

**[schieber@blankrome.com](mailto:schieber@blankrome.com)**

**[slifer@blankrome.com](mailto:slifer@blankrome.com)**

# Table of Contents

- Privacy: Gramm-Leach-Bliley Act Overview (# 3-4)
- Financial Privacy Rule (# 5)
- Consumers and Customers (#6-7)
- Consumers (#8)
- Customers (#9)
- Types of Notices (#10-11):
- Revised Notices (#12)
- Delivery of Privacy Notice (#13)
- Opt-Out Rights (#14-15)
- Non-Existent Consumer Opt-Out Rights (#16-17)
- Safeguards Rule (#18)
- Who Must Comply (#19)
- How to Comply (#20-25)
- Employee Management and Training (#26-29)
- Information Systems (# 30-32)
- Records Destruction (#33-35)
- Managing System Failures (#36)
- Vendor Contracts (#37-38)
- Cross Border Connections (#39)
- Security Breaches (#40-41)
- Security Breaches – Third Party Vendor Issues (#42-45)

# Privacy: Gramm-Leach-Bliley Act Overview

- More than six years have passed since the Gramm-Leach-Bliley Act (the "Act" or "GLBA") became effective on July 1, 2001.
- The Act, which is noted primarily for overhauling the financial services regulatory environment in order to allow one-stop shopping for banking and insurance services under the same roof, imposed many burdensome obligations on financial institutions to protect consumers' financial information.

# Privacy: Gramm-Leach-Bliley Act Overview

- GLBA applies to "financial institutions" - companies that offer financial products or services to individuals, like mortgage loans, financial or investment advice, or insurance.
- The Federal Trade Commission has authority to enforce the law with respect to "financial institutions" that are not covered by the federal banking agencies, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and state insurance authorities.
- Among the institutions that fall under FTC jurisdiction for purposes of the GLBA are non-bank mortgage lenders and servicers, loan brokers, some financial or investment advisers, and certain other providers of real estate settlement services.

- In a nutshell, the Privacy Rule requires financial institutions to:
  - (1) provide notices to consumers regarding the financial institution's practices regarding the sharing of nonpublic personal information; and
  - (2) disclose to consumers that they have the right to prevent the financial institution from sharing nonpublic personal information about the consumer in some situations.
- The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies who receive such information.
- Businesses need to make operational and technical changes to ensure that consumers' nonpublic personal information will be protected in the ways actually described in the businesses' privacy policies and notices.

- A company's obligations under the Act depend on whether the company has consumers or customers who obtain its services.

- Why is the difference between consumers and customers so important? Because only customers are entitled to receive a financial institution's privacy notice automatically.
- Consumers are entitled to receive a privacy notice from a financial institution only if the company shares the consumers' information with companies not affiliated with it, with some exceptions.
- Customers must receive a notice every year for as long as the customer relationship lasts.

- *Definition:* A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

## **Example of Consumer Relationship:**

- Applying for a loan

- *Definition:* A "customer" is a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship with a consumer.

## **Example of Establishing a Customer Relationship:**

- Obtaining a loan from a mortgage lender

## Types of Notices:

- 1. *Initial*: To customers not later than when relationship is established; To consumers prior to sharing nonpublic personal information
- 2. *Opt-Out*: To consumers and customers prior to sharing information
- 3. *Short-Form*: To consumers who are not customers, in lieu of full initial notice, prior to sharing nonpublic personal information about them

## Types of Notices:

- 4. *Simplified*: To customers if don't share nonpublic personal information about current or former customers with affiliates or nonaffiliated third parties outside exceptions 313.14 and 313.15
- 5. *Annual*: To customers for duration of the relationship
- 6. *Revised*: To consumers, customers, and former customers

- If you change your privacy practices such that the most recent privacy notice you provided to a consumer is no longer accurate (e.g., you disclose a new category of nonpublic personal information or to a new nonaffiliated third party outside of specific exceptions and those changes are not adequately described in your prior notice), you must provide revised privacy and opt-out notices.

- The privacy notice must be given to individual customers or consumers by mail or in-person delivery; it may not, for example, be posted on a wall.
- Reasonable ways to deliver a notice may depend on the type of business the institution is in: for example, an online lender may post its notice on its website and require online consumers to acknowledge receipt as a necessary part of a loan application.
- By combining the annual privacy notice with other notices or mailings that go out to customers, including, for example, promotional pieces, businesses may save on postage, printing and staff costs.

- Consumers and customers have the right to opt out of - or say no to - having their information shared with certain third parties. The privacy notice must explain how - and offer a reasonable way - they can do that.
- For example, providing a toll-free telephone number or a detachable form with a pre-printed address is a reasonable way for consumers or customers to opt out; requiring someone to write a letter as the only way to opt out is not.
- If a consumer sends an opt-out notice to a business directing that the consumer's nonpublic personal information not be shared with third parties (unless of course, an exception applies that allows the information to be shared despite the opt-out), the business must have a system in place to ensure that the opt-out will be effective.

- The Act provides no opt-out right in several situations: For example, an individual cannot opt out if:
  - a financial institution shares information with outside companies that provide essential services such as data processing or servicing;
  - the disclosure is legally required;
  - a financial institution shares customer data with outside service providers that market the financial company's products or services.

- One interesting development that arose after the July 1, 2001 GLBA compliance deadline, is that some consumers attempted to assert nonexistent opt-out rights.
- Many businesses have received consumer opt-outs in cases where the business is not a financial institution covered under the Act, or if covered under the Act, where the financial institution indicated that it was not disclosing information outside of exceptions under the Act, so that no opt-out right existed.
- Many public interest groups attempted to educate consumers about their privacy rights, and some groups disseminated opt-out forms for consumers to fill out and send to all of the companies with which they do business.

- If a business voluntarily agrees to comply with a consumer request, where no legal obligation exists to do so, the business must take steps to ensure that the consumer's information is protected, or run the risk of being sued for breach of contract.
- If a business chooses not to comply with the consumer's request, the business should devise a diplomatic response identifying the reasons the consumer's request will not be honored.

- Financial institutions collect personal information from their customers, such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Act requires financial institutions to ensure the security and confidentiality of this type of information.
- The Safeguards Rule, enforced by the Federal Trade Commission and other regulators, requires financial institutions to have a security plan to secure and protect the confidentiality and integrity of personal consumer information.

- The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers. This includes mortgage lenders and their servicers.
- The Safeguards Rule requires financial institutions to design, implement and maintain safeguards to protect customer information.
- In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.
- The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to institutions such as credit reporting agencies and other third parties that receive customer information from financial institutions.

- The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information.
- The plan must be appropriate to the financial institution'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 financial institution must:

- Designate one or more employees to coordinate the safeguards;
- 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 appropriate service providers and contract with them to implement safeguards; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

- These requirements are designed to be flexible. Each financial institution should implement safeguards appropriate to its own circumstances.
- For example, some financial institutions may choose to describe their safeguards programs in a single document, while others may memorialize their plans in several different documents, such as one to cover an information technology division and another to describe the training program for employees.
- Similarly, a company may decide to designate a single employee to coordinate safeguards or may spread this responsibility among several employees who will work together.

- In addition, a firm with a small staff may design and implement a more limited employee training program (more on this below) than a firm with a large number of employees.
- A financial institution that doesn't receive or store any information online may take fewer steps to assess risks to its computers than a firm that routinely conducts business online.

- When a firm implements safeguards, the Safeguards Rule requires it to consider all areas of its operation, including three areas that are particularly important to information security: **employee management and training; information systems; and managing system failures.** Firms should consider implementing the following practices in these areas.

- The success or failure of your information security plan depends largely on the employees who implement it. You may want to:
  - Check references prior to hiring employees who will have access to customer information.
  - Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.

- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
  - locking rooms and file cabinets where paper records are kept;
  - using password-activated screensavers;
  - rapid screen lock-outs;
  - using strong passwords (e.g., eight characters long);
  - restricting cell phone cameras;
  - restricting iPods;

- changing passwords periodically, and prohibiting the posting of passwords near employees' computers;
- encrypting sensitive customer information when it is transmitted electronically over networks or stored online;
- referring calls or other requests for customer information to designated individuals who have had safeguards training; and
- recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.

- Instruct and regularly remind all employees of your organization's policy - and the legal requirement - to keep customer information secure and confidential.
- Provide employees with a detailed description of the kind of customer information you (they) handle (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored.
- Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.
- Impose disciplinary measures for breaches.

- Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on how to maintain security throughout the life cycle of customer information - that is, from data entry to data disposal:
  - Store records in a secure area. Make sure only authorized employees have access to the area. For example:

- store paper records in a room, cabinet, or other container that is locked when unattended;
- ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
- store 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;

- don't store sensitive customer data on a machine with an Internet connection;
- maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area; and
- use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.

- Document destruction rule.
  - any entity that uses “consumer reports” in establishing a consumer’s eligibility for credit, employment, insurance or other purposes must dispose of the information properly to protect against unauthorized access.
- Dispose of customer information in a secure manner. For example:
  - hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;

## Paper:

- Implementation of policies and procedures that require completely destroying paper:
  - Burning
  - Pulverizing
  - Shredding
  - Completely destroying papers so they cannot be read or reconstructed

## Electronic Media:

- Implementation of policies and procedures that require destruction of electronic media

# Records Destruction

- If contract with third party to dispose of and destroy the information, reasonable due diligence must be performed
- Implementation of policies and procedures against unauthorized or unintentional disposal

- Maintain a close inventory of your computers.
- check with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
- use anti-virus software that updates automatically;
- maintain up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations;
- address stolen, lost consumer data;
- technology changes may be necessary to prevent security breaches on the Internet.

- If a financial institution is disclosing nonpublic personal information about a consumer to a third party which is providing services to the financial institution, including, for example, marketing and servicing, the financial institution must contractually require that the third party maintain the confidentiality of any shared information.

- If a financial institution already had a contract in place with a vendor by July 1, 2000, the Act provided a grandfathering period until July 1, 2002, for the financial institution to enter into a new contract that provided a confidentiality provision.
- However, for new contracts entered into after July 1, 2000, the Act mandates that the confidentiality provisions be part of the contract.
- Whether or not required by federal law, data owners/licensees benefit from contractual provisions obligating vendors as such provisions
  - can serve to evidence due care
  - can facilitate data owner/licensee compliance with state data breach notification laws
- Vendors benefit, too
  - Establishes concrete, predictable obligations owed to data owner/licensee

## International Issues

- Off-shore outsourcing
  - Laws where data originated
  - Laws where data processed
- Vendor accountability
- EU
- Canada
- Others

## **Federal rule for banks requires implementing a response program that includes:**

- Notification of regulator
- Assessment of incident
- Taking appropriate steps to contain and control the incident
- Notification to customers when breach has occurred or is reasonably possible

## Varying state notification requirements

### State laws - Security breaches

- Not consistent
- Non-public personal information
- Risk test vs. Trigger test
- Manner of notification
- Notification of law enforcement
- Examples and Responses
- Business and public relations considerations
- Involvement of law enforcement

- **Practical Contracting Tips:**

- Define “security breach” (can be narrower or broader than applicable legal requirement)
- Vendor must notify data owner/licensee of breaches; must do so timely and with all details
- Vendor to cooperate with and assist data owner/licensee and law enforcement; to include assisting owner/licensee with breach notices, obtaining owner/licensee approval for all vendor notices
- Automatic amendment of vendor obligations to comply with changes to applicable law

- Responsibility for Breach Notification – Who Has It?
- Structure/Form of Breach Notification
- Vendor issues under state and federal statutes and regulations
- Vendor contractual issues
- Vendor relationship concerns

# Security Breaches – Third Party Vendor Issues

- State security breach notification laws – a sampling
  - Vendor reporting obligations
- “Any business ... that compiles or maintains computerized records ... on behalf of another business ... shall notify that business ... of any breach of security of the computerized records immediately following discovery” (N.J.S. § 56:8-163(b))
- “A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data” (73 P.S. § 2303(c))
- A commercial entity that maintains computerized data that includes personal information that ... the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data immediately following discovery of a breach. (6 Del. C. § 12B-102(b))

- Federal security laws (financial institutions)
  - Institution requirements
    - Each financial institution “shall ... [r]equire its service providers by contract to implement appropriate measures designed to meet the objectives of [the Interagency Guidelines Establishing Information Security Standards]” (Interagency Guidelines, § III.D.2.)
    - “[A]n institution’s contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution’s customer information, including notification to the institution as soon as possible of any such incident” (Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, § II)

Document No. 21606521v1