

# **The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information**

**Prepared By: James Michael Kemp  
© Copyright 2005 – All rights reserved**

---

## **I. INTRODUCTION**

The Gramm-Leach-Bliley Act (“GLB Act”) was enacted on November 19, 1999, and is codified at 15 U.S.C. § 6801, et seq. Federal implementing regulations may be found at 16 C.F.R. § 313, et seq., which became effective with respect to the notice requirements on November 13, 2000, and with a required compliance date of July 1, 2001. A full analysis of this law is beyond the scope of this seminar, but attention should be directed to Subtitle A of Title V of the GLB Act, which contains the privacy provisions relating to consumers' financial information. Under these provisions, financial institutions have restrictions on when they may disclose a consumer's personal financial information to nonaffiliated third parties. All financial institutions are further required by the GLB Act to provide notices to their customers about their information-collection and information-sharing practices and the opportunity to “opt out” before disclosing information to nonaffiliated third parties. Consumers have the right to “opt out” or prevent the sharing of their information with nonaffiliated third parties in most circumstances. However, the GLB Act does provide specific exceptions under which a financial institution may share customer information with a third party and the consumer has no right to “opt out”.

The GLB Act further establishes what is known as the “Safeguards Rule” for all personal information collected by financial institutions. Simply put, the GLB Act requires all financial institutions to ensure the security and confidentiality of a customer's personal information by implementing “administrative, technical and physical safeguards”. See 15 U.S.C 6801(b), 6505(b)(2); 16 C.F.R. § 314, et seq.

---

## **II. KEY CONCEPTS**

### **A. Financial Institutions**

A “financial institution” is any institution which is engaged in the business or realm of financial activities as described in section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)), which will be subject to the requirements of the GLB Act. However, under the Final Rule promulgated by the Federal Trade Commission (FTC), an institution must be significantly engaged in financial activities to be considered a “financial institution.”

As examples, the following specific practices fall under the definition of financial activities:

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities; insuring, guaranteeing, or indemnifying against loss, harm, damage, illness,

disability, or death; providing financial investment or economic advisory services; underwriting or dealing with securities. [§ 4(k)(4)(A-E)]

- Engaging in an activity that the Federal Reserve Board has determined to be closely related to banking. [§ 4(k)(4)(F); 12 C.F.R. § 225.28].

Examples:

- Extending credit and servicing loans
- Real estate and personal property appraising
- Credit bureau services
- Real estate settlement services (i.e. closing, title search or exams, document preparation, notary or signing services, document preparation)
- Property or title insurance policies

## **B. Mortgage Brokers**

Mortgage brokers are financial institutions because the act of brokering mortgage loans is a financial activity referenced in section 4(k)(4)(F) of the Bank Holding Company Act and listed in 12 C.F.R. § 225.28(b)(1). See 15 U.S.C. § 6809(3); 16 C.F.R. § 313.3(k)(2)(xi). Mortgage brokers are subject to the FTC's enforcement authority, its Privacy Rule, and its Safeguards Rule. See 15 U.S.C. § 6805(a)(7); 16 C.F.R. § 313.1(b). The Privacy Rule applies when individuals seek your assistance in obtaining mortgage loans that are primarily for personal, family, or household purposes. Under the Privacy Rule, you establish a customer relationship when an individual enters into an agreement or understanding with you whereby you undertake to arrange or broker a residential mortgage loan for him or her. See 16 C.F.R. § 313.3(i)(2)(i)(E). You also establish a customer relationship when an individual provides any personally identifiable financial information to you in an effort to obtain a residential mortgage loan through you. See 16 C.F.R. § 313.4(c)(3)(i)(E).

## **C. Consumers**

*Definition:* A "consumer" is an individual or that individual's legal representative 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.

### **General Obligations to Consumers:**

- Provide an initial (or "short-form") notice about the availability of the privacy policy if the financial institution shares information outside the permitted exceptions.
- Provide an opt-out notice, with the initial notice or separately, prior to a financial institution sharing nonpublic personal information with nonaffiliated third parties.
- Provide consumers with a "reasonable opportunity" to opt out before disclosing nonpublic personal information about them to nonaffiliated third parties, such as 30 days from the date the notice is mailed.
- If a consumer elects to opt out of all or certain disclosures, a financial institution must honor that opt-out direction as soon as is reasonably practicable after the opt-out is received.
- 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 NPI to a new nonaffiliated third party outside of specific exceptions and those changes are not adequately described in your prior notice), you must provide new revised privacy and opt-out notices.

## **D. Customers**

*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.

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

- Providing personally identifiable financial information to a broker in order to obtain a mortgage loan
- Obtaining a loan from a mortgage lender
- Agreeing to obtain tax preparation or credit counseling services

*"Special Rule" for Loans:* The customer relationship travels with ownership of the servicing rights.

- A financial institution establishes a customer relationship with a consumer when it originates a loan.
- If it subsequently sells the loan and retains the servicing rights, it continues to have a customer relationship with the consumers.
- If it subsequently transfers the servicing rights, the entity that acquires servicing has a customer relationship with the consumer.
- Those with an ownership interest in the loan but without servicing rights have consumers.

### **General Obligations to Customers**

- Provide an initial privacy notice not later than when the customer relationship is established.
- Provide, with the initial privacy notice or separately, an opt-out notice prior to sharing nonpublic personal information with nonaffiliated third parties outside of specific exceptions.
- Provide an annual privacy notice annually for the duration of the customer relationship.
- Provide customers with a "reasonable opportunity" to opt out before disclosing nonpublic personal information about them to nonaffiliated third parties, such as 30 days from the date the notice is mailed.
- NOTE: If a customer elects to opt out of all or certain disclosures, a financial institution must honor that opt-out direction as soon as reasonably practicable after the opt-out is received.
- 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 NPI 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 new revised privacy and opt-out notices.

## **E. Nonpublic Personal Information ("NPI")**

**NPI Includes:**

- Nonpublic personally identifiable financial information; and
- Any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.
- Specific Examples of NPI
  1. Social security numbers
  2. Drivers license numbers
  3. Credit reports
  4. Mortgage loan or bank account information
  5. HUD-1 settlement statements
  6. Sales contracts
  7. Mortgage loan or application documents

**NPI Excludes:**

- Publicly available information; and
- Any list, description or other grouping of consumers (including publicly available information pertaining to them) that is derived without using personally identifiable financial information that is not publicly available.

**"Personally Identifiable Financial Information" is any information:**

- A consumer provides to obtain a financial product or service;
- About a consumer resulting from any transaction involving a financial product or service; or
- Otherwise obtained about a consumer in connection with providing a financial product or service.

**"Publicly Available Information" is:**

- Any information that a financial institution has a *reasonable basis to believe* is lawfully made available to the general public from:
  - Federal, State, or local government records;
  - Widely distributed media; or
  - Disclosures to the general public required by Federal, State, or local law.

**"Reasonable Basis to Believe" means the financial institution:**

- Cannot assume information is publicly available.
- Must take steps to determine if:
  - the information is of the type generally made available to the public;
  - whether an individual can direct that it not be made available; and
  - if so, whether that particular consumer has directed that it not be disclosed.

**Examples of Publicly Available Information:**

- Fact that an individual is a mortgage customer of a particular financial institution where that fact is recorded in public real estate records
- Telephone number listed in the phone book
- Information lawfully available to the general public on a website (including a website that requires a password or fee for access)

**Examples of NPI (assuming such information is not publicly available):**

- Fact that an individual is the customer of a particular financial institution
- Consumer's name, address, social security number, account number
- Any information a consumer provides on an application
- Information from a "cookie" obtained in using a website
- Information on a consumer report obtained by a financial institution (NOTE: Such information may also be covered by the Fair Credit Reporting Act)

**NPI and Lists:** Always consider how the list is derived.

- List of a finance company's mortgage customers with their outstanding mortgage balance and account numbers is NPI
- List of a retailer's credit card customers is NPI
- List of a retailer's credit card customers that is combined with a list of magazine subscribers is NPI
- List of all individuals who purchased washing machines from a retailer is NOT NPI where the information is not derived from information obtained in providing a financial product or service

## **F. Notices**

**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
4. *Simplified:* To customers if don't share NPI 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

**Format of Notices: Notices Must Be "Clear and Conspicuous"**

1. "Clear and conspicuous" means that a notice must be reasonably understandable *and* designed to call attention to the nature and significance of the information in the notice.
2. "Reasonably understandable" means clear and concise sentences, plain language, active voice.

3. "Designed to call attention" means using headings, easily read typeface and type size, wide margins. On website: use text or visual cues to encourage scrolling down the page to view the entire notice; place notice on a frequently accessed page or via a clearly labeled link; ensure that there are no distracting graphics or sound.

**Content of Initial and Annual Notices:**

[for purposes of this section, "consumers" includes "customers"]

1. Categories of nonpublic personal information that the financial institution collects, for example:

- information obtained from the consumer
- information obtained from the consumer's transactions with a financial institution or its affiliate
- information obtained from nonaffiliated third parties about the consumer's transactions with them
- information obtained from a consumer reporting agency

2. Categories of nonpublic personal information that the financial institution discloses. Must provide illustrative examples, such as:

- information from the consumer on applications or other forms, such as name, address, and social security number
- information from transactions with the consumer: account number and balances, payment history, parties to transactions, credit card usage
- information from a consumer reporting agency: creditworthiness and credit history

3. Categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information. Must provide illustrative examples, such as:

- Financial service providers, such as mortgage brokers and insurance companies
- Non-financial companies, such as magazine publishers, retailers, and direct marketers
- Others, such as nonprofit organizations

4. If the financial institution discloses nonpublic personal information about former customers:

- Categories of nonpublic personal information disclosed; and
- Categories of affiliates and nonaffiliated third parties to whom nonpublic personal information is disclosed (other than what is permitted under exceptions 313.14 and 313.15).

5. If the financial institution discloses nonpublic personal information to a nonaffiliated third-party under exception 313.13 (for service providers and joint marketing partners):

- Separate statement of the categories of nonpublic personal information disclosed (including illustrative examples); and

- Statement about whether the third party is:
    - a service provider that performs marketing services on behalf of the financial institution itself or on behalf of products or services jointly marketed between two financial institutions; or
    - another financial institution with whom the financial institution has entered into a joint marketing agreement.
6. An explanation of the consumer's right to opt out.
7. Any disclosures that the financial institution is required to make under the Fair Credit Reporting Act.
8. The financial institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.
9. If the financial institution discloses nonpublic personal information to a nonaffiliated third party under exceptions 313.14 and 313.15, state that disclosures to nonaffiliated third parties are made as permitted by law.
10. The financial institution may also reserve the right to disclose categories of nonpublic personal information that it does not currently disclose or categories of nonaffiliated third parties to which it does not currently disclose nonpublic personal information.

#### **Content of Opt-out Notice**

[for purposes of this section, "consumers" includes "customers"]

1. Fact that the financial institution discloses (or reserves the right to disclose) nonpublic personal information about a consumer to nonaffiliated third parties.
2. The consumer's right to opt out of those disclosures.
3. A description of a "reasonable means" by which the consumer can opt out, for example:
  - Toll-free telephone number
  - Detachable form with mailing information
  - If the consumer has agreed to receive notices electronically, an electronic means such as a form that can be sent via e-mail or through the financial institution's website
  - NOTE: It is NOT a reasonable means to require a consumer to write her own letter as the ONLY option

*Remember:* A financial institution must allow a "reasonable opportunity" for the consumer to opt out before sharing information.

#### **Content of the Short-Form Notice**

1. State that the financial institution's full privacy policy is available on request.
2. Explain a reasonable means by which the consumer may obtain the full notice, for example:

- Toll-free telephone number
- On-site for in-person transactions

### **Content of Simplified Notice**

1. List the categories of NPI collected.
2. Provide statement explaining that the institution does not share NPI with affiliates and nonaffiliated third parties, except as permitted by law (if applicable).
3. Provide statement explaining the institution's policies and practices with respect to safeguarding NPI.

### **Revised Notice**

If a financial institution changes its policies and practices regarding disclosure of nonpublic personal information to nonaffiliated third parties outside of specific exceptions, it must:

- Provide a new notice that accurately reflects its policies; and
- Provide a new opt-out notice and a reasonable means to opt out.

### **Timing of Annual Notice**

- Financial institution must provide an accurate privacy policy to its customers at least annually during the continuation of the customer relationship.
- Annually means at least once in a period of twelve consecutive months which the financial institution can define but must apply consistently. A financial institution can send annual notices to all its customers at the same time each year.
  - Customer opens account in January of 2004. Financial institution must send its first annual notice to that customer by December 2005.

### **Delivery of Notices**

- Consumer or customer must be reasonably expected to receive actual notice in writing or, if the customer agrees, electronically. Examples of appropriate delivery include:
  - Hand delivery
  - Mail to last known address
  - For a consumer using an ATM, post the notice on the screen and require acknowledgment of receipt of the notice as a necessary part of the transaction.
  - For the consumer who conducts transactions electronically, post the notice on the website and require acknowledgment of receipt of the notice as a necessary part of the transaction.
  - For the customer who uses a website for electronic financial transactions and agrees to receive an annual notice at that website, post the current privacy notice continuously in a clear and conspicuous manner on that website.
  - The notice CANNOT just be posted in a branch or on a website.

- Customers must be provided notice in a form that can be retained or accessed at a later time.

## **G. Exceptions**

A financial institution may disclose nonpublic personal information to nonaffiliated third parties under several exceptions where consumers and customers do not have the right to opt out of such sharing and, in some cases, will get no notice of the disclosure.

### **Section 313.13**

- Financial institution must provide notice but not the right to opt out when it provides nonpublic personal information to:
  - Third party service provider that provides services for the financial institution; or
  - Other financial institution(s) with whom the financial institution has entered into a joint marketing agreement.
- Third party service provider may market the financial institution's own products and services or the financial products or services offered under a "joint marketing agreement" between the financial institution and one or more other financial institutions.
- Joint marketing agreement with other financial institution(s) means a written contract pursuant to which those institutions jointly offer, endorse, or sponsor a financial product or service.
- To take advantage of this exception the financial institution must:
  - Provide the initial notice as required to consumers and customers; and
  - Enter into a contract with the third party service provider or financial institution under a joint marketing agreement that prohibits the disclosure or use of the information other than for the purpose for which it was disclosed.

### **Exception 313.14:**

- Disclosures *necessary to effect, administer, or enforce a transaction* that a consumer requests or authorizes (see section 313.14(b)); or
- Disclosures made in connection with:
  - Servicing or processing a financial product or service that a consumer requests or authorizes
  - Maintaining or servicing a consumer's account
  - A proposed or actual securitization, secondary market sale (including the sale of servicing rights) or similar transactions

### **Exception 313.15:**

- With consumer consent
- To protect the confidentiality or security of records
- To protect against or prevent actual or potential fraud
- For required institutional risk control or for resolving consumer disputes or inquires

- To persons holding a legal or beneficial interest relating to the consumer
- To persons acting in a fiduciary or representative capacity on behalf of the consumer (i.e., the consumer's attorney)
- To provide information to insurance rate advisory organizations, persons assessing compliance with industry standards, the financial institution's attorneys, accountants or auditors
- To law enforcement entities or self-regulatory groups (to the extent permitted or required by law)
- To comply with Federal, State, or local laws
- To comply with subpoena or other judicial process
- To respond to summons or other requests from authorized government authorities
- Pursuant to the Fair Credit Reporting Act, to a consumer reporting agency or from a consumer report reported by consumer reporting agency
- In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit

---

### **III. SAFEGUARDS RULE**

The “Safeguards Rule” applies to any business that is significantly engaged in providing financial products or services to consumers (see discussion of “financial institutions” above), as well as an affiliate or service provider of the financial institution that may receive customer information in the course and scope of their work. All financial institutions must develop a written information security plan that sets forth their program to protect customer information.

A plan need only be appropriate to the size and complexity of the financial institution, the nature and scope of activities engaged in, and the amount and sensitivity of customer information processed. As part of this plan, each financial institution must:

1. Designate one or more employees to coordinate the safeguards;
2. Identify and assess the risks to customer information in each area of operations;
3. Evaluate the effectiveness of the current safeguards for controlling these risks;
4. Design and implement a safeguards program, and regularly monitor and test the program;
5. Select appropriate service providers and contract with them to implement their own safeguards; and
6. Evaluate and adjust the Safeguards Program in light of relevant circumstances, changes in the company’s business arrangements or service providers, or the results of the monitoring of the current safeguards.

The stated objective of the Safeguards Rule is to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security and integrity of customer information, and protect against unauthorized access or use of customer information.

Any Safeguards Program must start with employee management and training. Employers may want to adequately investigate employees before hiring and implement a written contract or employment agreement setting forth the duty of confidentiality of customer information. Employees should be trained on physical and electronic safekeeping of all personal information, regardless of its form. Paper and files may be locked in appropriate storage areas with limited access. Computers and related data should be password and software protected, to prevent both internal and external breaches of security. Employees should be aware of fraudulent phone calls or other improper attempts (often referred to as a "pretext") that occurs in an effort to obtain customer information. Lastly, all customer information must be disposed of in an appropriate manner, which may include shredding important papers and destroying any electronic storage device (i.e. disk drives) that may contain personal information.

---

#### **IV. CONCLUSION**

State laws are not pre-empted by the GLB Act except to the extent that they are "inconsistent" with this federal law. As with most federal laws, a state law addressing privacy issues will not be deemed "inconsistent" if it affords "greater protection" to consumers than provided for by the federal law. Real estate professionals are advised to investigate the state specific laws in their jurisdiction of practice to determine whether any additional regulations apply to their particular activity. In addition, it is important to remember that businesses engaging in one of the listed financial activities are not always required to provide their customer with a privacy notice under the GLB Act. The notice obligations depend on whether the business is providing a financial product or service to customers or to what extent they share a customer's information with nonaffiliated third parties outside of specific exceptions. Secondly, it is prudent, under the GLB Act and for general liability reasons, to discuss and implement a written plan with all employees of your organization detailing the scope of the information protected, as well as all policies or procedures in place to prevent unauthorized disclosure of a customer's personal information.

See Exhibit below for an example of a Privacy Notice under the GLB Act.

**ALTA SAMPLE PRIVACY FORM  
Revised August 28, 2001**

**[Insert name of title insurer or agent]**

**Privacy Policy Notice**

**PURPOSE OF THIS NOTICE**

Title V of the Gramm-Leach-Bliley Act (GLBA) generally prohibits any financial institution, directly or through its affiliates, from sharing nonpublic personal information about you with a nonaffiliated third party unless the institution provides you with a notice of its privacy policies and practices, such as the type of information that it collects about you and the categories of persons or entities to whom it may be disclosed. In compliance with the GLBA, we are providing you with this document, which notifies you of the privacy policies and practices of **[insert name of institution and its affiliates mentioned in this notice]**

We may collect nonpublic personal information about you from the following sources:

Information we receive from you such as on applications or other forms.

Information about your transactions we secure from our files, or from [our affiliates or] others.

Information we receive from a consumer reporting agency.

Information that we receive from others involved in your transaction, such as the real estate agent or lender.

Unless it is specifically stated otherwise in an amended Privacy Policy Notice, no additional nonpublic personal information will be collected about you.

We may disclose any of the above information that we collect about our customers or former customers to our affiliates or to nonaffiliated third parties as permitted by law.

We also may disclose this information about our customers or former customers to the following types of nonaffiliated companies that perform services on our behalf or with whom we have joint marketing agreements:

1. Financial service providers such as companies engaged in banking, consumer finance, securities and insurance.
2. Non-financial companies such as envelope stuffers and other fulfillment service providers.

**WE DO NOT DISCLOSE ANY NONPUBLIC PERSONAL INFORMATION ABOUT YOU WITH ANYONE FOR ANY PURPOSE THAT IS NOT SPECIFICALLY PERMITTED BY LAW.**

We restrict access to nonpublic personal information about you to those employees who need to know that information in order to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

The ALTA sample privacy form includes a full list of the requisite disclosures. The sample form does not envision sharing of information outside the corporate title insurance underwriter and affiliate or agent structure. If you are considering sharing nonpublic customer information and do not qualify for an exception within the Federal Trade Commission and/or state rules, please obtain legal advice on what should be included in your form.