

FEDERAL TRADE COMMISSION

**BUREAU OF CONSUMER PROTECTION
DIVISION OF FINANCIAL PRACTICES**

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

Subtitle A of Title V of the Gramm-Leach-Bliley Act (“GLB Act”) has 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. Financial institutions are required to provide notices to their customers about their information-collection and information-sharing practices. Consumers may decide to “opt out” if they do not want their information shared with nonaffiliated third parties. The GLB Act provides specific exceptions under which a financial institution may share customer information with a third party and the consumer may not opt out. All financial institutions are required to provide consumers with a notice and opt-out opportunity before they may disclose information to nonaffiliated third parties outside of what is permitted under the exceptions.

Subtitle A of Title V of the GLB Act and the Federal Trade Commission regulation can be found on the Gramm-Leach-Bliley Act web page which can be reached directly from the FTC home page at www.ftc.gov.

I. Important Dates and Citations about the Gramm-Leach-Bliley Act

Statute (Public Law 106-102, 15 U.S.C. § 6801, et seq.)

- enacted November 12, 1999

Regulations (16 C.F.R. § 313, 65 Fed. Reg. 33646 (May 24, 2000))

- effective date: November 13, 2000
- compliance date: July 1, 2001

• **Other Agencies’ Rules**

- Federal Reserve Board: 12 C.F.R. § 216
- OTS: 12 C.F.R. § 573
- OCC: 12 C.F.R. § 40
- FDIC: 12 C.F.R. § 332
- NCUA: 12 C.F.R. § 716
- SEC: 17 C.F.R. § 248
- CFTC: 17 C.F.R. § 160

** The views expressed in this presentation are not the official views of the Federal Trade Commission or of any individual Commissioner. June 18, 2001.*

II. Overview

A. Key Definitions

- Financial Institution
- Consumers and Customers
- Nonpublic Personal Information

B. Notices

C. Exceptions

D. Limits on Reuse and Redisclosure

III. Financial Institution

Definition: Any institution the business of which is engaging in *financial activities* as described in *section 4(k) of the Bank Holding Company Act* (12 U.S.C. § 1843(k)). 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.”

A. 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]. For example:
 - Extending credit and servicing loans
 - Collection agency services
 - Real estate and personal property appraising
 - Check guaranty services
 - Credit bureau services
 - Real estate settlement services
 - Leasing real or personal property (on a nonoperating basis for an initial lease term of at least 90 days)
- Engaging in an activity that a bank holding company may engage in outside of the United States. [§ 4(k)(4)(G); 12 C.F.R. § 211.5(d)]. For example:
 - Operating a travel agency in connection with financial services

- Only those activities determined to be financial activities under § 4(k)(1-3) as of November 12, 1999, are covered by the FTC Privacy Rule. While the Federal Reserve Board and the Department of Treasury have authority to add activities that are “incidental” or “complementary” to financial activities, the FTC will review those determinations before proposing to extend coverage of its Rule to such new activities.

B. Examples of businesses that engage in “financial activities” and are “financial institutions” for purposes of the GLB Act¹:

- Mortgage lender or broker
- Check casher
- Pay-day lender
- Credit counseling service and other financial advisors
- Medical-services provider that establishes for a significant number of its patients long-term payment plans that involve interest charges
- Financial or investment advisory services including tax planning, tax preparation, and instruction on individual financial management
- Retailer that issues its own credit card
- Auto dealers that lease and/or finance
- Collection agency services
- Relocation service that assists individuals with financing for moving expenses and/or mortgages
- Sale of money orders, savings bonds, or traveler’s checks
- Government entities that provide financial products such as student loans or mortgages

C. “Significantly Engaged” in Financial Activities:

- Whether a financial institution is “significantly engaged” in financial activities is a flexible standard that takes into account all the facts and circumstances.
- Examples of businesses that are not “significantly engaged” for purposes of the GLB Act:
 - Retailer that does not issue its own credit card (even if it accepts other credit cards)
 - Grocery store that allows consumers to get cash back by writing a check in an amount higher than the actual purchase price

¹ Even if a business engages in one of these financial activities, it does not necessarily have to provide privacy notices. The notice obligations depend on whether the business is providing a financial product or service to customers or, if they share the information with nonaffiliated third parties outside of specific exceptions, to consumers.

- Merchant who allows an individual to “run a tab”
- Retailer that provides occasional “lay-away” and deferred payment plans or accepting payment by means of credit cards issued by others as its only means of extending credit

IV. Consumers and Customers

A. Consumers

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.

Examples of Consumer Relationships:

- Applying for a loan
- Obtaining cash from a foreign ATM, even if it occurs on a regular basis
- Cashing a check with a check-cashing company
- Arranging for a wire transfer

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.

B. 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:

- Opening a credit card account with a financial institution
- Entering into an automobile lease (on a non-operating basis for an initial lease term of at least 90 days) with an automobile dealer
- 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.

V. 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.

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

VI. Notices

A. 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

B. 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.

C. 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.

D. 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.

E. 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

F. 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.

G. 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.

H. 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.

I. 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.

VII. 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.

A. Exception to Opt-Out Requirements: 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.

B. Exceptions to Notice and Opt-Out Requirements: Sections 313.14 and 313.15

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

VIII. Limits on Reuse and Redisclosure by a Third Party

These restrictions apply to a third party that receives nonpublic personal information from a nonaffiliated financial institution.

- A. Reuse and Rediscovery Under Exception 313.13:** Information received under section 313.13 is restricted by the confidentiality agreement required under that section and cannot be used except for the purpose for which it was disclosed.
- B. Reuse and Rediscovery Under Exceptions 313.14 and 313.15:**
When a third party receives nonpublic personal information from a nonaffiliated financial institution under exception 313.14 or 313.15, the third party may:
- Disclose the information to affiliates of the financial institution from whom it received the information; or
 - Disclose the information to its own affiliates who are limited in their use and disclosure of the information to the same extent as the third party; or
 - Disclose and use the information pursuant to exceptions 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception for which it was received.
- C. Reuse and Rediscovery Outside of Exceptions 313.14 and 313.15:**
Where a third party receives nonpublic personal information from a financial institution outside of an exception (after the financial institution has provided notice and opt out and the consumer has not opted-out), the third party may:
- Disclose the information to the affiliates of the financial institution from whom it received the information; or
 - Disclose the information to its own affiliates, who are limited in their use of information in the same manner as the third party; or
 - Disclose the information to any other entity consistent with the privacy policy of the financial institution from which it received the information.
- D. Examples of Limits on Reuse and Rediscovery:**
A third party receives information from a financial institution to process account transactions authorized by consumers (pursuant to a section 313.14 exception):
- That third party may disclose that information to other nonaffiliated third parties in the ordinary course of business to carry out the servicing.
 - It may also disclose it in response to a properly authorized subpoena.
 - It *may not* use the information for its own marketing or sell it to another entity for marketing.
- A magazine publisher purchases a list of a financial institution's customers (those who have not opted-out) where the disclosure falls outside the exceptions:
- It may use that list for its own purposes.
 - It may disclose that list to other nonaffiliated third parties consistent with the financial institution's privacy policy.

IX. Other Issues

- A. Prohibition on Sharing Account Numbers for Marketing Purposes**

Financial institutions may not disclose, directly or through an affiliate, an account number of a consumer's credit card account, bank account, or transaction account to a nonaffiliated third party for use in marketing. A transaction account is an account to which a third party can initiate charges.

Exceptions:

- Disclosure to a consumer reporting agency.
- Disclosure to an agent or service provider to perform marketing of the financial institution's own products or services, provided that the agent or service provider is not authorized to directly initiate charges to the account.
- Disclosure to a participant in a private label credit card program or an affinity program where the participants are identified to the customer when the customer enters into the program.
- Disclosure of an encrypted account number to a nonaffiliated third party, provided that the financial institution does not give the third party the means to decode the number or code.

B. Effect on the Fair Credit Reporting Act

The FCRA is expressly not modified, limited, or superseded by Subtitle A of Title V of the GLB Act.

C. Relationship to State Laws:

State laws are not preempted except to the extent that they are "inconsistent" with this federal law. A state law is not "inconsistent" if it affords "greater protection" to consumers than provided for by this federal law, as determined by the FTC.