

**The Winn Brown Law Firm, PLLC**

Winn Davis Brown, Jr., Attorney At Law, Ext. 106  
Board Certified - Creditors' Rights Specialist  
American Board of Certification

Winn Davis Brown, III, Attorney At Law, Ext. 105  
Collection Manager - *Debbie W. McClain, Ext. 103*  
Collection Paralegals: - *Jamie D. Holland, Ext. 107*  
*Paula N. Owston, Ext. 109*  
*Audra M. Montague, Ext. 108*  
Accounting - *Randy Neal, Ext. 101*

Clerk of Appellate Courts  
P.O. Box 249  
Jackson, MS 39205

**FILED**

**JUN 11 2020**

Re: Motion to Amend Rule 11 of the Mississippi Rules of Civil Procedure.

OFFICE OF THE CLERK  
SUPREME COURT  
COURT OF APPEALS

**We oppose the requirement to include the filer's email address on all filed items.**

This requirement will cause compliance problems when dealing with pro se consumer litigants.

The inclusion of the email address will lead the pro se consumer litigant to think that email is an appropriate means of communication, when due to privacy concerns as detailed in MEC, the FDCPA, Consumer Financial Protection Bureau regulations, Gramm-Leach-Bliley Act, and other regulatory requirements regarding Non-public Personal Information email is NOT an appropriate means for communication with pro se consumer litigants. See attachment.

A law firm dealing with pro se consumer litigants must avoid email communication regarding Non-public Personal Information, if for no other reason than *the law firm has no control over to whom the pro se consumer litigant will transmit the law firm's email response which may contain Non-public Personal Information.*

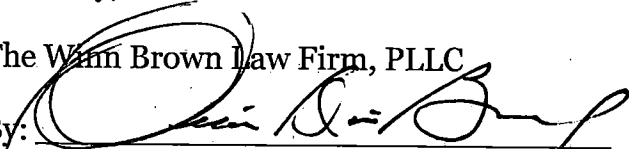
Note: we did not oppose the email address requirement on discovery materials because we perceive the risk as less in that context than in the context of pleadings.

Although we speak from the context of the often overlooked yet numerous collection cases that form the vast majority of the civil cases filed in the circuit and county courts, we perceive this as a great risk to the plaintiff's bar as a whole.

Aside from the email address requirement, we do not oppose the proposed rule otherwise.

Cordially,

The Winn Brown Law Firm, PLLC

By:   
Winn Davis Brown, Jr.

By:   
Winn Davis Brown, III



**MOTION#**

2020

407

The Winn Brown Law Firm, PLLC  
P. O. Box 249, 1613 Main St.  
Southaven, MS 38671  
Phone: (662) 393-9466 / (800) 737-9466  
Fax: (662) 393-7600  
E-mail: [winn.brown@winnfirm.com](mailto:winn.brown@winnfirm.com)

June 8, 2020



## FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS


---

# How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act

**TAGS:** [FinTech](#) | [Privacy and Security](#) | [Gramm-Leach-Bliley Act](#) | [Finance](#) | [Real Estate and Mortgages](#)

**RELATED RULE:** [Financial Privacy Rule](#)

Financial institutions covered by the Gramm-Leach-Bliley Act must tell their customers about their information-sharing practices and explain to customers their right to "opt out" if they don't want their information shared with certain third parties. Is your company following the requirements of the Privacy Rule?

 [View PDF \(98.78 KB\)](#)

---

## ABOUT THE GLB ACT

The Gramm-Leach-Bliley Act was enacted on November 12, 1999. In addition to reforming the financial services industry, the Act addressed concerns relating to consumer financial privacy. The Gramm-Leach-Bliley Act required the Federal Trade Commission (FTC) and other government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions (GLB Act). The regulations required all covered businesses to be in full compliance by July 1, 2001.

The FTC is responsible for enforcing its Privacy of Consumer Financial Information Rule (Privacy Rule). Anyone who uses this Guide should also review the Privacy Rule, found at [16 C.F.R. Part 313](#) (May 24, 2000).

## TABLE OF CONTENTS

### INTRODUCTION

#### I. WHO IS COVERED BY THE PRIVACY RULE

Are you a financial institution?

Do you have consumers or customers?

What information is covered?

Businesses That Receive NPI from Nonaffiliated Financial Institutions.

## **II. YOUR OBLIGATIONS UNDER THE PRIVACY RULE**

### Privacy Notices

#### Who Gets a Privacy Notice?

- Customers
- Consumers Who Are Not Customers

#### The Contents of the Privacy Notice

#### The Appearance of the Privacy Notice

#### Safeguarding NPI

#### Delivering Privacy Notices

#### Opt-Out Notices

- General Obligations
- Exercising the Opt-Out Right
- The Shelf Life of an "Opt-Out" Direction
- Summary Of Notice Requirements

#### Exceptions

- Exceptions to the Notice and Opt-Out Requirements
- Exception to the Opt-Out Requirement: Service Providers and Joint Marketing

## **III. LIMITS ON REUSE AND REDISCLOSURE OF NPI**

### General Obligations

Restrictions on Reuse and Redisclosure if NPI is Received Under the Section 14 or 15 Exceptions.

Restrictions on Reuse and Redisclosure if NPI is Received Outside the Section 14 or 15 Exceptions.

## **IV. DISCLOSURE OF ACCOUNT NUMBERS IS PROHIBITED**

## **V. OTHER ISSUES**

### The Fair Credit Reporting Act

### Enforcement

## **VI. FURTHER GUIDANCE**

# **INTRODUCTION**

The Gramm-Leach-Bliley Act seeks to protect consumer financial privacy. Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties. The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions because they engage in certain "financial activities." Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they don't want their information shared with certain nonaffiliated third parties. In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information.

An overview of the privacy requirements of the GLB Act is available [online](#). This guide provides more detailed information than in the overview, to help you comply with the Privacy Rule's requirements for protecting consumer financial

information. It was written for businesses that provide financial products or services to individuals for personal, family, or household use.

[\[back to Table of Contents\]](#)

# I. WHO IS COVERED BY THE PRIVACY RULE

There are two ways that the Privacy Rule might cover you. First, if you are a "financial institution," you are covered. Parts I and II of this guide describe your obligations if you collect "nonpublic personal information" from your "customers" or "consumers" and define these terms. Second, if you receive "nonpublic personal information" from a financial institution with which you are not affiliated, you may be limited in your use of that information. Part III of this guide discusses your obligations as a recipient of such protected information.

## Are you a "financial institution"?

The Privacy Rule applies to businesses that are "significantly engaged" in "financial activities" as described in section 4(k) of the Bank Holding Company Act. Your activities determine whether you are a "financial institution" under the Privacy Rule. According to the Bank Holding Company Act provision and regulations established by the Federal Reserve Board, "financial activities" include:

lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders.

providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors.

brokering loans.

servicing loans.

debt collecting.

providing real estate settlement services.

career counseling (of individuals seeking employment in the financial services industry).

These examples are taken from the [section 4\(k\) provisions and regulations on financial activities](#).

Under the Privacy Rule, only an institution that is "significantly engaged" in financial activities is considered a financial institution. You need to take into account all the facts and circumstances of your financial activities to determine if you are "significantly engaged" in such activities. The FTC's "significantly engaged" standard is intended to exclude certain activities that might otherwise fall under the Privacy Rule. Two factors are particularly important in determining whether you are "significantly engaged" in a financial activity. First, is there a formal arrangement? A storeowner or bartender who "runs a tab" for customers is not considered to be significantly engaged in financial activities, but a retailer that offers credit directly to consumers by issuing its own credit card would be covered. Second, how often does the business engage in a financial activity? A retailer that lets some consumers make payments through an occasional lay-away plan is not "significantly engaged" in a financial activity. In contrast, a business that regularly wires money to and from consumers is significantly engaged in a financial activity.

## Do you have consumers or customers?

If you are a financial institution, your obligations depend on whether your clients are "customers" or "consumers." In brief, the Privacy Rule requires you to give notice to all of your "customers" about your privacy practices, and, if you share their information in certain ways, to your "consumers" as well.

Under the Rule, a "consumer" is someone 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 person's legal representative. The term "consumer" does not apply to commercial clients, like sole proprietorships. Therefore, where your client is not an individual, or is an individual seeking your product or service for a business purpose, the Privacy Rule does not apply to you.

### Examples of "consumer" relationships:

---

- cashing a check with a check-cashing company
- making a wire transfer
- applying for a loan, whether or not you actually obtain the loan

"Customers" are a subclass of consumers who have a continuing relationship with a financial institution. It's the nature of the relationship - not how long it lasts - that defines your customers. Even if an individual repeatedly uses your services for unrelated transactions, she may not be your "customer." For example, if an individual uses the ATM at a bank where she does not have an account, those isolated transactions, no matter how frequent, do not make her that bank's customer. She would still be a "consumer" of that bank, however.

A former customer "has obtained" a financial product or service from a financial institution but no longer has a continuing relationship with it. For purposes of your obligations under the Privacy Rule, a former customer is considered to be a consumer.

### Examples of "customer" relationships:

---

- opening a credit card account with a financial institution
- leasing an automobile from an auto dealer
- using the services of a mortgage broker to secure financing
- obtaining the services of a tax preparer or investment adviser
- getting a loan from a mortgage lender or payday lender

### A Word About Customer Relationships and Loans

---

A special rule defines the customer relationship when several financial institutions participate in a loan transaction. A financial institution establishes a customer relationship with an individual when it originates a loan. If the financial institution sells the loan but maintains the servicing rights, it continues to have a customer relationship with the individual. If the financial institution transfers the servicing rights but retains an ownership interest in the loan, the individual is a "consumer" of that institution and a "customer" of the institution with the servicing rights. If other institutions hold an ownership interest in the loan (but not the servicing rights), the individual is their consumer, too.

## What information is covered?

The Privacy Rule protects a consumer's "nonpublic personal information" (NPI). NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available."

**NPI is:**

any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);

any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or

any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

NPI does not include information that you have a reasonable basis to believe is lawfully made "publicly available." In other words, information is not NPI when you have taken steps to determine:

that the information is generally made lawfully available to the public; and

that the individual can direct that it not be made public and has not done so.

For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, her phone number would not be "publicly available."

**Publicly Available Information Includes:**

---

federal, state, or local government records made available to the public, such as the fact that an individual has a mortgage with a particular financial institution.

information that is in widely distributed media like telephone books, newspapers, and websites that are available to the general public on an unrestricted basis, even if the site requires a password or fee for access.

Information in a list form may be NPI, depending on how the list is derived. For example, a list is not NPI if it is drawn entirely from publicly available information, such as a list of a lender's mortgage customers in a jurisdiction that requires that information to be publicly recorded. Also, it is not NPI if the list is taken from information that isn't related to your financial activities, for example, a list of individuals who respond to a newspaper ad promoting a non-financial product you sell.

But a list derived even partially from NPI is still considered NPI. For example, a creditor's list of its borrowers' names and phone numbers is NPI even if the creditor has a reasonable basis to believe that those phone numbers are publicly available, because the existence of the customer relationships between the borrowers and the creditor is NPI.

**Putting It All Together:**

---

**Examples of Nonpublic Personal Information (in list form)**

list of a retailer's credit card customers

list of a payday lender's customers

list of auto loan customers merged with list of car magazine subscribers

## Businesses That Receive NPI from Nonaffiliated Financial Institutions.

Even if your business is not a financial institution that has consumers or customers, the Privacy Rule may limit your use of NPI. Your ability to reuse and redisclose the information may be restricted if you receive NPI from a nonaffiliated financial institution. It depends on why you receive it (see "[LIMITS ON REUSE AND REDISCLOSURE OF NPI](#)").

[\[back to Table of Contents\]](#)

## II. YOUR OBLIGATIONS UNDER THE PRIVACY RULE

### Privacy Notices.

Financial institutions must give their customers - and in some cases their consumers - a "clear and conspicuous" written notice describing their privacy policies and practices. When you provide the notice and what you say depend on what you do with the information.

### Who Gets a Privacy Notice?

#### Customers

Whether or not you share customer NPI, you must give all your customers a privacy notice. You must provide an "initial notice" by the time the customer relationship is established. If this would substantially delay the customer's transaction, you may provide the notice within a reasonable time after the customer relationship is established, but only if the customer agrees.

If you share NPI with nonaffiliated third parties outside of the exceptions described within (see "[Exceptions](#)"), you also must give your customers:

- an "opt-out" notice explaining the individual's right to direct you not to share her NPI with a nonaffiliated third party;
- a reasonable way to opt out; and
- a reasonable amount of time to opt out before you disclose her NPI.

You must also give your customers an "annual notice" - a copy of your full privacy notice - for as long as the customer relationship lasts.

#### Consumers Who Are Not Customers

Before you share NPI with nonaffiliated third parties outside of the exceptions described within (see "[Exceptions](#)"), you must give your non-customer consumers a privacy notice, including an opt-out notice. If you don't share information with nonaffiliated third parties, or if you only share within the exceptions, you do not have to give a privacy notice to your consumers.

If you are required to provide a privacy notice to your consumers, you may choose to give them a "short-form notice" instead of a full privacy notice. The short-form notice must:

- explain that your full privacy notice is available on request;
- describe a reasonable way consumers may get the full privacy notice; and

include an opt-out notice.

## The Contents of the Privacy Notice

Your notice must accurately describe how you collect, disclose, and protect NPI about consumers and customers, including former customers. Your notice must include, where it applies to you, the following information:

Categories of information collected. For example, nonpublic personal information obtained from an application or a third party such as a consumer reporting agency.

Categories of information disclosed. For example, information from an application, such as name, address, and phone number; Social Security number; account information; and account balances.

Categories of affiliates and nonaffiliated third parties to whom you disclose the information. For example, financial services providers, such as mortgage brokers and insurance companies; or non-financial companies, such as magazine publishers, retailers, direct marketers, and nonprofit organizations. You also may describe categories of other nonaffiliated parties to whom you may disclose NPI in the future.

Categories of information disclosed and to whom under the joint marketing/ service provider exception in section 313.13 of the Privacy Rule (see "**Exceptions**").

If you are disclosing NPI to nonaffiliated third parties under the exceptions in sections 313.14 (exceptions for processing or administering a financial transaction) and 313.15 (exceptions, including fraud prevention or complying with federal or state law and others) of the Privacy Rule (see "**Exceptions**"), a statement that the disclosures are made "as permitted by law."

If you are disclosing NPI to nonaffiliated third parties, and that disclosure does not fall within any of the exceptions in sections 313.14 and 313.15, an explanation of consumers' and customers' right to opt out of these disclosures (see "**Opt-Out Notices**").

Any disclosures required by the Fair Credit Reporting Act (see "**Fair Credit Reporting Act**").

Your policies and practices with respect to protecting the confidentiality and security of NPI (see "**Safeguarding NPI**").

You only need to address those items listed above that apply to you. For example, if you don't share NPI with affiliates or nonaffiliated third parties except as permitted under sections 313.14 and 313.15, you can provide a simplified notice that: (1) describes your collection of NPI; (2) states that you only disclose NPI to nonaffiliated third parties "as permitted by law;" and (3) explains how you protect the confidentiality and security of NPI.

## The Appearance of the Privacy Notice

The privacy notice must be "clear and conspicuous," whether it is on paper or on a website. It must be reasonably understandable, and designed to call attention to the nature and significance of the information. The notice should use plain language, be easy to read, and be distinctive in appearance. A notice on a website should be placed on a page that consumers use often, or it should be hyperlinked directly from a page where transactions are conducted.

## Safeguarding NPI

The FTC has issued a separate rule to address the requirements for safeguarding NPI. See 16 C.F.R. Part 314, 67 Fed. Reg. 36484 (May 23, 2002). You should consult the FTC's website for more information about this rule and further guidance for small businesses in implementing the Safeguards Rule requirements.

The Privacy Rule requires that your privacy notice provide an accurate description of your current policies and practices with respect to protecting the confidentiality and security of NPI. For example, if you restrict access to NPI to employees who need the information to provide products or services to your consumers or customers, say so.



## Delivering Privacy Notices

You must deliver your privacy notices to each consumer or customer in writing, or, if the consumer or customer agrees, electronically. Your written notices may be delivered by mail or by hand. For individuals who conduct transactions with you electronically, you may post your privacy notice on your website and require them to acknowledge receiving the notice as a necessary part of obtaining a particular product or service. For annual notices, you may reasonably expect that your customers have received your notice if they use your website to access your financial products or services and agree to receive notices at your website, and you post your notice continuously in a clear and conspicuous manner on your website.

Notices given orally or posted in your office(s) don't comply with the rule.

## Opt-Out Notices

### General Obligations

If you share their NPI with nonaffiliated third parties outside of three exceptions (see "**Exceptions**"), you must give your consumers and customers an "opt-out notice" that clearly and conspicuously describes their right to opt out of the information being shared. An opt-out notice must be delivered with a privacy notice, and it can be part of the privacy notice.

The opt-out notice must describe a "reasonable means" for consumers and customers to opt out. They must receive the notice and have a reasonable opportunity to opt out before you can disclose their NPI to these nonaffiliated third parties. Acceptable "reasonable means" to opt out include a toll-free telephone number or a detachable form with a check-off box and mailing information. Requiring the consumer or customer to write a letter as the only option is not a "reasonable means" to opt out.

**Note:** While the GLB Act does not require you to provide an opt-out notice if you only disclose NPI to affiliates, if you share certain information with your affiliates, you may have an obligation to provide an opt-out notice under the Fair Credit Reporting Act. That opt-out notice must be included in your GLB privacy notice (see "**Fair Credit Reporting Act**").

### Exercising the Opt-Out Right

You must give consumers and customers a "reasonable opportunity" to exercise their right to opt out, for example, 30 days, after you send the initial notice either on- or off-line, before you can share their information with nonaffiliated third parties outside the exceptions. For an isolated consumer transaction, like buying a money order, you may require your consumers to make their opt-out decision before completing the transaction.

Consumers and customers who have the right to opt out may do so at any time. Once you receive an opt-out direction from your existing consumers or customers, you must comply with it as soon as is reasonably possible.

### The Shelf Life of an Opt-Out Direction

An opt-out direction by a consumer or customer is effective - even after the customer relationship is terminated - until canceled in writing, or, if the consumer agrees, electronically. However, if a former customer establishes a new customer relationship with you and you are required to provide an opt-out notice, the customer must make a new opt-out direction that will apply only to the new relationship.

## SUMMARY OF NOTICE REQUIREMENTS

Initial

Customers

Not later than when you establish the customer relationship, unless it would substantially delay the transaction and the customer agrees

Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)

Consumers who are not customers (including former customers)

Before you disclose their NPI to a nonaffiliated third party outside of certain exceptions

Full description of information-collection and sharing practices or "short-form" notice, along with opt-out notice

Annual

Customers

Delivery on a consistent basis at least once in any period of 12 consecutive months for the duration of the customer relationship

Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)

## Exceptions

### Exceptions to the Notice and Opt-Out Requirements

There are a number of exceptions to the notice and opt-out requirements. These exceptions are located in sections 313.14 ("section 14 exceptions") and 313.15 ("section 15 exceptions") of the Privacy Rule. If you share information only under these sets of exceptions, you don't need to give your consumers a privacy notice, but you will need to give your customers a simplified initial and, if applicable, an annual privacy notice. Customers and consumers have no right to opt out of these disclosures of NPI.

The section 14 exceptions apply to various types of information-sharing that are necessary for processing or administering a financial transaction requested or authorized by a consumer. This includes, for example, disclosing NPI to service providers who help mail account statements and perform other administrative activities for a consumer's account. It also includes disclosures to and by creditors listed by a consumer on a credit application to perform a credit check.

The section 15 exceptions apply to certain types of information-sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws. Examples of appropriate information disclosures under this exception include those made to technical service providers who maintain the security of your records; your attorneys or auditors; a purchaser of a portfolio of consumer loans you own; and a consumer reporting agency, consistent with the Fair Credit Reporting Act (see "[Exceptions](#)").

### Exception to the Opt-Out Requirement: Service Providers and Joint Marketing

Another exception can be found in section 313.13 ("section 13 exception") of the Privacy Rule. If you share information under this exception, you must give your customers - and your consumers if you share their information - a privacy notice that describes this disclosure. However, your consumers and customers do not have a right to opt out of this information sharing.

The section 13 exception covers disclosures for certain service providers and for certain marketing activities. The section 13 exception covers disclosures to third party service providers whose services for you do not fall within the section 14 exceptions. For example, if you hire a nonaffiliated third party to provide services in connection with marketing your products or to market financial products jointly for you and another financial institution, or to do a general analysis of your customer transactions, your disclosure of NPI for these purposes does not fall under the section 14 exceptions. Therefore, you can use the section 13 exception for these types of service providers.

The section 13 exception also applies to marketing financial products or services offered through a "joint agreement" with one or more other financial institutions. The "joint agreement" requirement means that you have entered into a written contract with one or more financial institutions about your joint offering, endorsement, or sponsorship of a financial product or service. This does not apply to any kind of joint marketing you do, but only joint marketing with other financial institutions and only the marketing of financial products or services.

To take advantage of the section 13 exception, you must enter into a contract with those nonaffiliated third parties with whom you share NPI. The agreement must guarantee the confidentiality of the information by prohibiting the third party or parties from using or disclosing the information for any purpose other than the one for which it was received. Contracts with nonaffiliated service providers that are effective before July 1, 2000 and don't have the required confidentiality agreement must be amended to include such a provision by July 1, 2002.

### **III. LIMITS ON REUSE AND REDISCLOSURE OF NPI**

#### **General Obligations.**

If you receive NPI from a nonaffiliated financial institution, your ability to reuse and redisclose that information is limited. The limits depend on how the information is disclosed to you. It does not matter whether or not you're a financial institution.

#### **Restrictions on Reuse and Redisclosure if NPI is Received Under the Section 14 or 15 Exceptions**

You may receive NPI from a nonaffiliated financial institution ("originating financial institution") under the section 14 or 15 exceptions. In these situations, you may only disclose and use the information in the ordinary course of business to carry out the purpose for which it was received. That purpose may include disclosures to other parties under the section 14 or 15 exceptions in order to carry out that activity, or as otherwise necessary, such as to respond to a subpoena. You may also disclose the information to your affiliates, who are limited in their reuse and redisclosure of the information in the same way as you are, and to affiliates of the originating financial institution.

#### **Restrictions on Reuse and Redisclosure if NPI is Received Outside the Section 14 or 15 Exceptions**

Alternatively, you may receive NPI from a nonaffiliated financial institution outside the section 14 or 15 exceptions. For example, you may want to purchase a financial institution's customer list in order to market your own products to those individuals. In these cases, the originating financial institution may disclose NPI about those consumers or customers who were informed about this type of disclosure in the privacy notice, and who did not opt out after receiving notice and the opportunity to opt out.

In this situation, you may use the information internally for your own purposes. However, you may only redisclose the information consistent with the privacy policy of the originating financial institution. In other words, you step into the shoes of the originating financial institution and may disclose the same kinds of NPI to the same entities as the originating institution. For example, if the originating financial institution's privacy notice informed its consumers and customers that it would only share their NPI with "nonfinancial institutions, such as charitable organizations," you may redisclose the NPI to charitable institutions as well. However, because the originating institution does not disclose NPI to another financial institution, such as an insurance provider, you cannot because that type of company is not covered by the privacy policy.

You may also disclose the information to your affiliates, whose redisclosure is limited in the same way as you, and to affiliates of the originating financial institution.

[\*\*\[back to Table of Contents\]\*\*](#)

## IV. DISCLOSURE OF ACCOUNT NUMBERS IS PROHIBITED

The GLB Act prohibits financial institutions from sharing account numbers or similar access numbers or codes for marketing purposes. This prohibition applies even when a consumer or customer has not opted-out of the disclosure of NPI concerning her account. The prohibition applies to disclosures of account numbers for an individual's credit card account, deposit account, or "transaction account" to any nonaffiliated third party to use in telemarketing, direct mail marketing, or other marketing through electronic mail to any consumer. A "transaction account" is any account to which a third party may initiate a charge. This provision does not prohibit the sharing of an encrypted account number, if the third party receiving the information has no way to decode it.

This prohibition applies to the complete marketing transaction, including posting a charge to an account. However, it does not apply when you disclose an account number to your agent or service provider just to market your own products or services, as long as the party receiving the information can't directly initiate charges to the account.

The exceptions in sections 313.14 and 313.15 of the Privacy Rule do not apply to the disclosure of account numbers for marketing purposes. For example, you may not obtain your customer's consent to disclose her account number for marketing purposes.

[\[back to Table of Contents\]](#)

## V. OTHER ISSUES

### The Fair Credit Reporting Act

The Gramm-Leach-Bliley Act's notice and opt out provisions are in addition to the obligations imposed by the Fair Credit Reporting Act (FCRA). If the FCRA currently requires that you make clear and conspicuous disclosures to your consumers regarding your sharing of certain information (such as consumer report and application information) with your affiliates, you must continue to do so. The GLB Act requires these disclosures to be made as part of any privacy policy you give to your consumers or customers. See more information about the [FCRA and how it applies to your information sharing practices](#).

### Enforcement

The FTC, the federal banking agencies, (1) other federal regulatory authorities, (2) and state insurance authorities enforce the GLB Act. Each agency has issued substantially similar rules implementing GLB's privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance providers. The FTC has jurisdiction over any financial institution or other person not regulated by other government agencies.

The FTC may bring enforcement actions for violations of the Privacy Rule. The FTC can bring actions to enforce the Privacy Rule in federal district court, where it may seek the full scope of injunctive and ancillary equitable relief. The FTC also has authority under Section 5 of the FTC Act to examine privacy policies and practices for deception and unfairness.

[\[back to Table of Contents\]](#)

## VI. FURTHER GUIDANCE

See additional information about the [GLB Act](#) and the [Privacy Rule](#). Information available at that site will include written guidance, prepared by the staff of the FTC and other federal agencies enforcing the GLB Act, on specific compliance

issues that may be of interest to you.

[\[back to Table of Contents\]](#)

## FOOTNOTES

1. The Federal Reserve Board, the Office of Thrift Supervision, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation.
2. The National Credit Union Administration, the Securities and Exchange Commission, and the Commodity Futures Trading Commission.

## For More Information

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a [complaint](#) or to get [free information on consumer issues](#), visit [ftc.gov](http://ftc.gov) or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters consumer complaints into the [Consumer Sentinel Network](#), a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

## Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to [www.sba.gov/ombudsman](http://www.sba.gov/ombudsman).

July 2002



[ftc.gov](http://ftc.gov)