CONSUMER PRIVACY – IT’S THE LAW!

GRAMM/LEACH/BLILEY PRIVACY ACT

SANDI KRUISE INSURANCE TRAINING
4319 Corral Canyon Road
Bonita, CA 91902
800-517-7500
www.kruise.com

© 2003-2015 Sandi Kruise Insurance Training, Sandi Kruise Inc, All rights reserved.
# TABLE OF CONTENTS

## PRIVACY LAWS

- **Introduction** ................................................................. 4
- **History of Privacy Laws in Insurance** .......................... 4
- **The Gramm-Leach-Bliley (GLB) Act** .............................. 4
- **Key Features of GLBA for the Insurance Industry** .......... 5
  - **Title V of GLB** .......................................................... 5
- **Financial Institutions Include Insurance Agents** .......... 6
- **Consumers and Customers** .......................................... 6
- **The Privacy Notice** ...................................................... 7
- **Opt-Out Rights** .......................................................... 7
- **Receiving Nonpublic Personal Information** ................... 7
- **Other Provisions** .......................................................... 8
- **For More Information** .................................................. 8

## THE NAIC MODEL PRIVACY ACT

- **Privacy of Consumer Financial and Health Information Regulation** ........................................ 9
- **Table of Contents** ......................................................... 9
- **Table of Contents** ......................................................... 9

## BASIC REQUIREMENTS UNDER TITLE V OF GLB

## GENERAL PROVISIONS OF THE GLB ACT

- **Article I. General Provisions** ...................................... 12
- **Authority** ....................................................................... 12
  - **State Law** .................................................................. 12
- **Purpose and Scope** ...................................................... 12
- **Rule of Construction** .................................................... 13
- **Definitions** .................................................................... 13
  - **Affiliate** .................................................................... 13
  - **Clear and Conspicuous** ............................................. 14
  - **Collect** ....................................................................... 15
  - **Commissioner** .......................................................... 15
  - **Company** .................................................................. 15
  - **Consumer** .................................................................. 15
  - **Consumer reporting agency** .................................... 17
  - **Control** ....................................................................... 17
  - **Customer** ................................................................... 18
  - **Customer Relationship** .......................................... 18
  - **financial institution** .................................................. 19
  - **financial product or service** ..................................... 19
  - **health care** .............................................................. 20
  - **health care provider** .................................................. 20
  - **health information** .................................................... 20
  - **insurance product or service** .................................... 20
  - **licensee** ..................................................................... 21
  - **non-affiliated third party** ......................................... 22
  - **nonpublic personal information** ............................... 23
  - **nonpublic personal financial information** .................. 23
  - **nonpublic personal health information** ....................... 25
  - **personally identifiable financial information** .......... 25
  - **publicly available information** ................................. 27

© Copyright Sandi Kruise Insurance Training, 2004 all rights reserved 1
INTRODUCTION

This course provides information to help you comply with the Privacy Act's requirements protecting consumer financial information. It was written for businesses that provide financial products or services to individuals for personal, family, or household use, including insurance companies and agents.

Protecting the privacy of consumer information held by "financial institutions" is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999. The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information.

Currently both state and federal privacy laws regulate how financial institutions use or share consumer and customer data. This course summarizes the requirements of the most significant privacy laws affecting financial institutions and, specifically, the insurance industry:

- Title V of the Gramm-Leach-Bliley Act (GLBA)
- The Fair Credit Reporting Act (FCRA)
- The Electronic Fund Transfer Act (EFTA)
- The Right to Financial Privacy Act (RFPA)
- The Children's Online Privacy Protection Act (COPPA)

While the GLBA is the most extensive of the federal financial privacy laws, these other laws are also currently in full effect, and entities and their subsidiaries are expected to be in compliance with them and any applicable state privacy laws.

HISTORY OF PRIVACY LAWS IN INSURANCE

- In 1982, the NAIC (National Association for Insurance Commissioners) drafted the Insurance Information and Privacy Protection Model Act (hereinafter called The 1982 Privacy Act). Currently, 16 states have adopted language from this Act.

- In 1999, The Gramm/Leach/Bliley Act (GLB) was signed into law. GLB includes many key concepts of the of The 1982 Privacy Act.

- On September 26, 2000, the NAIC Adopted the Privacy of Consumer Financial and Health Information Model Regulation. The model regulation was drafted in response to requirements set forth in Title V of GLB. This was the state insurance regulators response to protecting the privacy of insurance consumers’ personal information.

THE GRAMM-LEACH-BLILEY (GLB) ACT

The GLB Act, also known as the Financial Services Modernization Act, was a long-awaited regulatory modernization bill for the financial services industry. Title V of the GLB Act sets
forward a stringent set of guidelines that restrict the use of consumer information by financial institutions.

The financial institutions covered by the GLB include entities and their financial and operating subsidiaries, as well as a wide range of other businesses engaged in financial and financially-related activities.

In addition to reforming the financial services industry, the Gramm-Leach-Bliley 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) be in full compliance by July 1, 2001.

The Agencies recently promulgated final rules to implement the GLB provisions. The GLB requirements became effective on November 13, 2000, and compliance with these requirements were mandatory as of July 1, 2001. To be in compliance with the regulations, prior to July 1, 2001, entities must have delivered copies of their privacy policies to their customers, and, as appropriate, provided them with a reasonable opportunity to opt out of certain information sharing arrangements between the entity and nonaffiliated third parties before such information sharing occurs.

KEY FEATURES OF GLBA FOR THE INSURANCE INDUSTRY

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.

TITLE V OF GLB

GLB is a federal law that was driven by the rampant telemarketing industry, the Internet, and people’s fears about identity theft. The GLB establishes a minimum federal standard that governs customer privacy for all financial institutions under Title V of GLB.

Title V of GLB the enacts specific legislation regarding the privacy of an individual’s personal data. The requirements of Title V apply to all financial institutions including insurance companies.

The Federal Reserve Board will supervise financial holding companies established under the Act, but generally must rely upon the examinations, reports, and decisions of the functional regulators.

GLB preserves the authority of each state to regulate the insurance industry. GLB allows the states to enact privacy legislation that is more restrictive than GLB, therefore providing greater privacy protection.
State insurance departments will be the functional regulators of the insurance business activities of all financial firms engaged in the business of insurance, including entities. As a result, the insurance industry faces the difficult challenge of complying with potentially different privacy laws in each of the 51 jurisdictions.

**Financial Institutions Include Insurance Agents**

The GLB Act applies to "financial institutions" - companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. As defined in GLB, independent insurance agents are financial institutions and must meet all of the basic privacy requirements. The law requires that financial institutions protect information collected about individuals; it does not apply to information collected in business or commercial activities.

Because of the impact the privacy laws have on agents, and the agent/company relationship, it is critical for all agents to understand their responsibilities under the privacy laws in the states in which they conduct business.

A Privacy Addendum will probably be added to most Agency Agreements, defining the steps each agent must take to assure compliance with the appropriate privacy laws.

Under the law, an agent may choose not to provide a privacy statement or opt-out if the insurer he or she represents provides the customer with the insurer's privacy statement and the agent does not share the customer's non-public personal information (NPPI) with anyone except the insurer or its affiliates.

Although agents are appointed to represent an insurance company, under the laws, they are still non-affiliated third parties to the insurer. As a result, an independent agent must be treated as a third party in determining what and when NPPI may be shared. And, as with all third party relationships, any sharing practice beyond the allowable exceptions must be defined in the company's privacy statement.

**Consumers and Customers**

A company’s obligations under the GLB Act depend on whether the individual who obtains its services is a consumer or customer. A **consumer** is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons. A **customer** is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long-term, the individual is deemed a customer of the institution.

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

Financial institutions must provide their customers with notices describing their privacy policies and practices, including their policies with respect to the disclosure of nonpublic personal information to their affiliates and to nonaffiliated third parties. The notices must be provided at the time the customer relationship is established and annually thereafter. Every entity must develop initial and annual privacy notices—even if they do not share information with nonaffiliated third parties.

The privacy notice must be given to individual customers or consumers by mail or delivered in-person. It may not be posted on a wall or published in a periodical. Reasonable ways to deliver a notice may depend on the type of business the institution is in: for example, an online entity may post its notice on its website and require online consumers to acknowledge receipt as a necessary part of accessing the site.

Opt-Out Rights

Consumers and customers have the right to opt out of - or say no to - having their information shared with certain third parties. The privacy notice must explain how - and offer a reasonable way - they can do that. For example, providing a toll-free telephone number or a detachable form with a pre-printed address is a reasonable way for consumers or customers to opt out; requiring someone to write a letter as the only way to opt out is not.

The privacy notice also must explain that consumers have a right to say no to the sharing of certain information - credit report or application information - with the company's affiliates. An affiliate is an entity that controls another company, is controlled by the company, or is under common control with the company. Consumers have this right under a different law, the Fair Credit Reporting Act. The GLB Act does not give consumers the right to opt out when companies share other information with its affiliates.

Receiving Nonpublic Personal Information

The GLB Act puts limits on how anyone that receives nonpublic personal information from a financial institution can use or re-disclose the information. If an entity discloses customer information to a service provider where the consumer has no right to opt out; the service provider may use the information for limited purposes. It may not sell or otherwise divulge the information to other organizations or use it for marketing.

However, when an entity receives nonpublic personal information from a financial institution that provided an opt-out notice -- and the consumer didn't opt out, the recipient’s financial institution may use the information for its own purposes or re-disclose it to a third party, consistent with the financial institution's privacy notice. If the privacy notice of the financial institution allows for disclosure to other unaffiliated financial institutions, such as an unaffiliated insurance provider, they may do so.

Traditional insurance providers will generally use the Act to offer their products through entities and other financial institutions and/or to become affiliated with an entity or other financial institution.
Other Provisions

Other important provisions of the GLB Act also impact how a company conducts business. For example, financial institutions are prohibited from disclosing their customers’ account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing or other marketing through e-mail, even if the individuals have not opted out of sharing the information for marketing purposes.

Another provision prohibits "pretexting" - the practice of obtaining customer information from financial institutions under false pretenses. The Federal Trade Commission (FTC) has brought several cases against information brokers who engage in pretexting.

For More Information

The FTC is one of eight federal regulatory agencies with the authority to enforce the financial privacy law, along with the state insurance authorities. The federal banking agencies, the Securities and Exchange Commission and the Commodity Futures Trading Commission have jurisdiction over banks, thrifts, credit unions, brokerage firms and commodity traders.

The FTC has additional details on the GLB Act, the Commission's Privacy Rule and a compliance guide for small business owners at [www.ftc.gov/privacy](http://www.ftc.gov/privacy).
THE NAIC MODEL PRIVACY ACT

Insurance companies and agents are regulated by the various Insurance regulators in each state. The NAIC has adopted a model Privacy Act which has been adopted by most, if not all states. Each state’s code should be reviewed however for differences from the model act. Throughout this course, the NAIC Model Privacy Act will be referenced. Text from the act itself will appear inside a box with explanations or discussion following some section.

© 2000 National Association of Insurance Commissioners Drafted: 9-20-00

PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION REGULATION

TABLE OF CONTENTS

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Authority
Section 2. Purpose and Scope
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

Section 5. Initial Privacy Notice to Consumers Required
Section 6. Annual Privacy Notice to Customers Required
Section 7. Information to be Included in Privacy Notices
Section 8. Form of Opt Out Notice to Consumers and Opt Out Methods
Section 9. Revised Privacy Notices
Section 10. Delivery

ARTICLE III. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 11. Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties
Section 12. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information
Section 13. Limits on Sharing Account Number Information for Marketing Purposes

ARTICLE IV. EXCEPTIONS TO LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 14. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing
Section 15. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions
Section 16. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information

ARTICLE V. RULES FOR HEALTH INFORMATION

Section 17. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 18. Authorizations
Section 19. Authorization Request Delivery
Section 20. Relationship to Federal Rules
Section 21. Relationship to State Laws

ARTICLE VI. ADDITIONAL PROVISIONS

Section 22. Protection of Fair Credit Reporting Act
Section 23. Nondiscrimination
Section 24. Violation
Section 25. Severability
Section 26. Effective Date

Appendix A –Sample Clauses
BASIC REQUIREMENTS UNDER TITLE V OF GLB

There are five basic requirements under Title V of GLB that agents must meet with respect to protecting non-public personal information (NPPI).

Insurers and agents are:

- Required to provide a clear, conspicuous disclosure of the entity’s privacy statement to all consumers and customers.

- Subject to specified exceptions, agents may not disclose nonpublic personal information about consumers to any nonaffiliated third party unless consumers are given a reasonable opportunity to direct that such information not be shared (to "opt out").

- Required to allow consumers and customers the right to “Opt-Out” if they share NPPI with third parties that do not fall within the business exceptions.

- Required to enter into a privacy agreement with non-affiliated third parties with whom they share NPPI under the processing and servicing exceptions which are discussed in a later section of this course.

- Prohibited from disclosing NPPI of consumers and customers to a non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail.

- Required to comply with new regulatory standards to protect the security and confidentiality (e.g. computers, hardcopy, encryption) of consumer's and customer's NPPI.
GENERAL PROVISIONS of THE GLB ACT

ARTICLE I. GENERAL PROVISIONS

AUTHORITY

SECTION 1. AUTHORITY
This regulation is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.

STATE LAW
A provision under a State law that provides greater consumer protection than provided under the GLBA privacy provisions will supersede the Federal privacy rule. The entity will be obligated to comply with the provisions of that State law to the extent those provisions provide greater consumer protection than the Federal privacy rule. The Federal Trade Commission determines whether a particular State law provides greater protection.

PURPOSE AND SCOPE

SECTION 2. PURPOSE AND SCOPE
A. Purpose. This regulation governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the state insurance department. This regulation:

(1) Requires a licensee to provide notice to individuals about its privacy policies and practices;

(2) Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and

(3) Provides methods for individuals to prevent a licensee from disclosing that information.

B. Scope. This regulation applies to:

(1) Nonpublic personal financial information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This regulation does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and
(2) All nonpublic personal health information.

C. Compliance. A licensee domiciled in this state that is in compliance with this regulation in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in such other state.

Drafting Note: Subsection 2C is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA’s privacy requirements.

RULE OF CONSTRUCTION

SECTION 3. RULE OF CONSTRUCTION

The examples in this regulation and the sample clauses in Appendix A of this regulation are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this regulation.

Agents should check the laws in their individual state for additional rates of construction and sample clauses.

DEFINITIONS

SECTION 4. DEFINITIONS

As used in this regulation, unless the context requires otherwise:

To understand the basic requirements of the privacy laws it is important to understand some basic terms. Learning the definitions will help you understand and comply with the privacy rule. This section provides an explanation of key terminology.

AFFILIATE

A. “Affiliate” means any company that controls, is controlled by or is under common control with another company.
An affiliate is any company that controls, is controlled by, or is under common control with another company. Thus, all subsidiaries of a parent company are "affiliates" of one another and the parent.

The privacy rule does not impose limitations on information sharing with affiliates. It does, however, require disclosure of such information sharing policies and practices. (The rules governing the sharing of information between an entity and its affiliates are set forth in the Fair Credit Reporting Act.)

**CLEAR AND CONSPICUOUS**

B. (1) “Clear and conspicuous” means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs, and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee’s notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:
(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the 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.

**COLLECT**

C. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

**COMMISSIONER**

D. "Commissioner" means the insurance commissioner of the state.

**Drafting Note:** Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

**COMPANY**

E. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

**CONSUMER**

F. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or
household purposes, and about whom the licensee has nonpublic personal information, or that individual’s legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee’s consumer.

(c) An individual who is a consumer of another financial institution is not a licensee’s consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee’s consumer if:

(i) (I) the individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) the individual is a claimant under an insurance policy issued by the licensee;

(III) the individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) the individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) the licensee discloses nonpublic personal financial information about the individual to a nonaffiliated third party other than as permitted under Sections 14, 15 and 16 of this regulation.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 5, 6 and 9 of this regulation to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, workers’ compensation plan participant, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about such an individual other than as permitted under Sections 14, 15 and 16 of this regulation, an individual is not the consumer of the licensee solely because he or she is:

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A beneficiary in a workers’ compensation plan.

**Drafting Note:** Regulators may wish to urge their workers’ compensation state insurance fund (or other applicable agency) to promulgate a regulation similar to this regulation in order to ensure parity in treatment of workers’ compensation plans and to ensure that all workers covered by such plans have privacy protections.
(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this Paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph(e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be customers for purposes of this regulation.

(g) An individual is not a licensee’s consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee’s consumer solely because he or she has designated the licensee as trustee for a trust.

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 a client is not an individual, or is seeking a product or service for a business purpose, the Privacy Rule does not apply. This could be someone who has submitted an application for a product, or someone who has an expired policy or contract.

The definition of consumer includes individuals who:

- **Apply for** a financial product or service for personal, family, or household purposes
- **Actually obtain** a financial product or service for personal, family, or household purposes

**CONSUMER REPORTING AGENCY**

G. “**Consumer reporting agency**” has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

These are entities such as Equifax and TRW who are used to obtain information.

**CONTROL**

H. “**Control**” means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or
(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

**CUSTOMER**

I. “Customer” means a consumer who has a customer relationship with a licensee.

A consumer becomes a customer at the time he/she enters into a continuing relationship with the company to provide a product that is to be used primarily for themselves or a family member, such as a Policyowner.

**CUSTOMER RELATIONSHIP**

J. (1) “Customer relationship” means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes.

(2) Examples.

(a) A consumer has a continuing relationship with a licensee if:

(i) The consumer is a current policyholder of an insurance product issued by or through the licensee; or

(ii) The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.

(b) A consumer does not have a continuing relationship with a licensee if:

(i) The consumer applies for insurance but does not purchase the insurance;

(ii) The licensee sells the consumer airline travel insurance in an isolated transaction;

(iii) The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;

(iv) The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;

(v) The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;

(vi) The customer’s policy is lapsed, expired, or otherwise inactive or dormant under the licensee’s business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than annual privacy
(vii) The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity; or

(viii) For the purposes of this regulation, the individual’s last known address according to the licensee’s records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

FINANCIAL INSTITUTION

K. (1) “Financial institution” means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);

(ii) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.); or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

Under the Privacy Rule, only an institution that is "significantly engaged" in financial activities is considered a financial institution.

FINANCIAL PRODUCT OR SERVICE

L. (1) “Financial product or service” means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution’s evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.
HEALTH CARE

M. "Health care" means:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:

(a) Relates to the physical, mental or behavioral condition of an individual; or

(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or

(2) Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.

Customers are a subset of consumers. A customer is a consumer with whom a company has a continuing relationship. Although the rule does not define "continuing relationship," it provides examples of transactions that are and are not considered continuing relationships.

HEALTH CARE PROVIDER

N. "Health care provider" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.

HEALTH INFORMATION

O. "Health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

INSURANCE PRODUCT OR SERVICE

P. (1) "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.
(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for an insurance product or service.

LICENSEE

Q. (1) “Licensee” means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state’s Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes, and cite appropriate state law.

(2) (a) A licensee is not subject to the notice and opt out requirements for nonpublic personal financial information set forth in Articles I, II, III and IV of this regulation if the licensee is an employee, agent or other representative of another licensee (“the principal”) and:

(i) The principal otherwise complies with, and provides the notices required by, the provisions of this regulation; and

(ii) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this regulation.

(b) Examples of employee, agent or other representative of a principal:

(i) An insurance broker, public adjuster or other licensee who is employed by another insurance broker, public adjuster or other licensee;

(ii) An independent adjuster adjusting a claim or benefit on behalf of an insurer;

(iii) An insurance agent of an insurer;

(iv) An insurance broker that has binding authority for an insurer; or

(v) A sublicensee of a licensee, whether or not the sublicensee is licensed in any other capacity.

(3) (a) Subject to Subparagraph (b), “licensee” shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state’s laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal financial information set forth in Articles I, II, III and IV of this regulation provided:
(i) The broker or insurer does not disclose nonpublic personal information of a consumer or a customer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 14 of this regulation, except as permitted by Section 15 or 16 of this regulation; and

(ii) The broker or insurer delivers a notice to the consumer at the time a customer relationship is established on which the following is printed in 16-point type:

**PRIVACY NOTICE**

“NEITHER THE U.S. BROKERS THAT HANDLED THIS INSURANCE NOR THE INSURERS THAT HAVE UNDERWRITTEN THIS INSURANCE WILL DISCLOSE NONPUBLIC PERSONAL INFORMATION CONCERNING THE BUYER TO NONAFFILIATES OF THE BROKERS OR INSURERS EXCEPT AS PERMITTED BY LAW.

**Drafting Note:** References to “excess lines broker” and “excess lines insurer” should be changed as necessary to correspond with the applicable terms used in each state.

The wording makes it clear that HMO’s are subject to this rule even if they are regulated by an entity other than the State Department of Insurance.

**NON-AFFILIATED THIRD PARTY**

R. (1) “Nonaffiliated third party” means any person except:

(a) A licensee’s affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee’s affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

A non-affiliated third party is any entity other than an affiliate or the company’s own employees.

The privacy rule restricts information sharing with nonaffiliated third parties. The rule defines nonaffiliated third parties as persons or entities except affiliates and persons jointly employed by
an entity and a nonaffiliated third party. Affiliates generally include an entity’s subsidiaries, its holding company, and any other subsidiaries of the holding company.

Although the privacy rule most commonly uses the term "nonaffiliated third parties," there are some instances in which a distinction is made between nonaffiliated financial institutions and all other nonaffiliated third parties. Readers should pay particular attention to these distinctions.

NONPUBLIC PERSONAL INFORMATION

Nonpublic personal information is the category of information protected by the privacy rule. The definitions for publicly available information and personally identifiable financial information work together to describe and define nonpublic personal information.

The privacy rule identifies three primary categories of information:

Non-Public vs. Public Information

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, that is not "publicly available."

NONPUBLIC PERSONAL FINANCIAL INFORMATION

T. (1) “Nonpublic personal financial information” means:

(a) Personally identifiable financial information; and

(b) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) Nonpublic personal financial information does not include:
(a) Health information;
(b) Publicly available information, except as included on a list described in Subsection T(1)(b) of this section; or
(c) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) Examples of lists.
(a) Nonpublic personal financial information includes any list of individuals’ names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.
(b) Nonpublic personal financial information does not include any list of individuals’ names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

NPI is any personally identifiable financial information that is:

- Provided by a consumer to a financial institution (e.g., name, address, or policy number).
- Any information an individual gives the entities to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
- Results from a transaction with the consumer (e.g., account balance information and payment history or information collected from the consumer via an Internet “cookie”).
- Any information about an individual from a transaction involving their financial product(s) or service(s) (for example, the fact that an individual is a consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- Otherwise obtained by the financial institution (e.g., customer status, MVR, or credit information).
- Any information about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

Nonpublic personal information, the category of information protected by the privacy rule includes:

- Personally identifiable financial information that is **not** publicly available information; and
• Lists, descriptions, or other groupings of consumers that were either

1. Created using personally identifiable financial information that is not publicly available information, or

2. Contain personally identifiable financial information that is not publicly available information.

A list is considered nonpublic personal information if it is generated based on customer relationships, loan balances, or other personally identifiable financial information that is not publicly available. A list is also considered nonpublic personal information if it contains any nonpublic personal information.

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 financial activities, for example, a list of individuals who respond to a newspaper ad promoting a non-financial product.

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.

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

NONPUBLIC PERSONAL HEALTH INFORMATION

U. “Nonpublic personal health information” means health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

Most information in a patient's medical file or an Insured's application and/or claims file would fall under this category.

PERSONALLY IDENTIFIABLE FINANCIAL INFORMATION
V. (1) “Personally identifiable financial information” means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable financial information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee’s customers or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee’s consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee’s consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable financial information does not include:

(i) Health information;

(ii) A list of names and addresses of customers of an entity that is not a financial institution; and

(iii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

**Personally identifiable financial information** is any information a entity collects about a consumer in conjunction with providing a financial product or service. This includes:

- Information provided by the consumer during the application process (e.g., name, phone number, address, income)
- Information resulting from the financial product or service transaction (e.g., payment history, loan or deposit balances, credit card purchases)
- Information from other sources about the consumer obtained in connection with providing the financial product or service (e.g., information from a consumer credit report or from court records)

**Personally identifiable financial information** also includes any information that "is disclosed in a manner that indicates that the individual is or has been your consumer." Thus, the very fact that an individual is a consumer of the entity is personally identifiable financial information.

**PUBLICLY AVAILABLE INFORMATION**

W. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee’s consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual’s telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.
**Publicly Available Information** (PAI) is any information that the institution has a reasonable basis to believe is lawfully made available to the general public from federal, state, or the local government, widely distributed media, or disclosures to the general public required by federal, state, or local government.

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.

The nature of the information, **not the source** of the information, determines whether it is publicly available information for purposes of the privacy rule. For example, even if an entity obtains customers' telephone numbers or the assessed value of their residences directly from the consumers, this information will be considered publicly available if the entity has a reasonable basis to believe the information could have been lawfully obtained from a public source. A reasonable belief exists if a entity has determined that (a) the information is of the type that is generally available to the public and (b) the individual has not blocked such information from public disclosure. This means, for example, that an entity can consider a customer's phone number to be publicly available, **but only** if the entity takes steps to determine the phone number is not unlisted.

It does not include information that you have a reasonable basis to believe is lawfully made "publicly available;" 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."

If information is not disclosed to non-affiliated companies outside the allowed business exception rules, it is not necessary to determine if information is public or non-public.
PRIVACY NOTICES

Under the GLBA, an entity must provide a notice that accurately describes its privacy policies and practices to individual consumers who establish a customer relationship with the entity, not later than the time the customer relationship is established. Unless an exception applies, this initial privacy notice also must be provided to any other consumer, even if not a "customer" of the entity, before the entity discloses that consumer’s nonpublic personal information to a nonaffiliated third party.

Entities also must provide their customers an annual privacy notice. All privacy notices must be clear and conspicuous, and must be provided so that each intended recipient can reasonably be expected to receive actual notice. Notices must be in writing (unless the consumer agrees to electronic delivery). The notices must describe, among other things, the types of nonpublic personal information collected and disclosed, the types of affiliated and nonaffiliated third parties with whom the information may be shared, and the consumer’s right to opt out and thereby limit certain information sharing by the entity.

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 the notice is provided and what it says depends on what agents do with the information.

The purpose of a privacy notice is to define their information sharing practices to the public.

ARTICLE II. PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

The following table reflects the rule’s requirements for delivering initial, annual, and revised notices to consumers and customers.

<table>
<thead>
<tr>
<th>Type of notice</th>
<th>Who gets it</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial privacy notice</td>
<td>• all existing bank customers</td>
<td>• no later than July 1, 2001</td>
</tr>
<tr>
<td>(all banks)</td>
<td>• all new bank customers after July 1, 2001</td>
<td>• when the customer relationship is established</td>
</tr>
<tr>
<td></td>
<td>• consumers who are not customers</td>
<td>• only if the bank intends to share nonpublic personal information about the consumer with a nonaffiliated third party</td>
</tr>
<tr>
<td>Annual privacy notice</td>
<td>• customers</td>
<td>• at least once in any period of 12 consecutive months while the customer relationship continues</td>
</tr>
<tr>
<td>(all banks)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revised privacy notice</td>
<td>• customers and consumers who are not customers</td>
<td>• before the bank shares nonpublic personal information in a manner not described in the most recent notice delivered to the customer or consumer</td>
</tr>
<tr>
<td>(as applicable)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
INITIAL PRIVACY NOTICE

SECTION 5. INITIAL PRIVACY NOTICE TO CONSUMERS REQUIRED

A. Initial notice requirement. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to:

The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most - or all - of the information a company has about them.

For example, nonpublic personal information could be information that a consumer or customer puts on an application; information about the individual from another source, such as a credit bureau; or information about transactions between the individual and the company, such as an account balance. Even the fact that an individual is a consumer or customer of a particular financial institution is nonpublic person information. But information that the company has reason to believe is lawfully public - such as mortgage loan information in a jurisdiction where that information is publicly recorded - is not restricted by the GLB Act.

The Privacy Notice must define its policies and procedures regarding the sharing and protection of non-public personal information. There are typically eight general parts that make up the content of the statement. These requirements may vary by state.

WHEN AND TO WHOM PRIVACY NOTICE MUST BE SENT

(1) Customer. An individual who becomes the licensee’s customer, not later than when the licensee establishes a customer relationship, except as provided in Subsection E of this section; and

(2) Consumer. A consumer, before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 15 and 16.

CUSTOMERS

CONSUMER VS. CUSTOMER

The privacy rule protects "consumers." All consumers receive the same privacy protections.
However, a subset of consumers defined as **customers** must receive certain disclosures, such as an annual privacy notice, that need not be provided to consumers who are not customers.

Obligations depend on whether clients are "customers" or "consumers." In brief, the Privacy Rule requires a notice to all "customers" about privacy practices, and, if their information is shared in certain ways, to "consumers" as well.

It is important to know the distinction between consumers and customers to understand the different disclosure requirements under the privacy rule.

Additional guidance regarding the customer relationship, found in the Supplemental Information (the preamble) of the rule, notes that a continuing relationship is established "where a consumer typically would receive some measure of continued service following, or in connection with, a transaction."

It's the nature of the relationship - not how long it lasts - that defines customers. Even an individual who repeatedly uses the entity's services for unrelated transactions may not be a "customer." Those isolated transactions, no matter how frequent, do not make someone an entity's customer. They would still be a "consumer" of that entity, 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 obligations under the Privacy Rule, a former customer is considered to be a consumer.

**The next diagram depicts the relationship between all individuals** who do business with an entity and those who meet the regulatory definitions for **consumers** and **customers**. As the diagram shows, only a portion of the individuals who conduct business with an entity are consumers under the privacy rule. Individuals are not considered consumers under this rule if they are commercial clients, grantors or beneficiaries of trusts for which the entity is trustee, or participants in an employee benefit plan that the entity sponsors.
B. When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection A(2) of this section if:

(1) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 15 and 16, and the licensee does not have a customer relationship with the consumer; or

(2) A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.

C. When the licensee establishes a customer relationship.

(1) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.

(2) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:

(a) Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or insurance broker, obtains insurance through that licensee; or

(b) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

D. Existing customers. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised policy notice, under Section 9, that covers the customer’s new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new privacy notice under Subsection A of this section.

E. Exceptions to allow subsequent delivery of notice.

(1) A licensee may provide the initial notice required by Subsection A(1) of this section within a reasonable time after the licensee establishes a customer relationship if:

(a) Establishing the customer relationship is not at the customer’s election; or

(b) Providing notice not later than when the licensee establishes a customer relationship would substantially delay the customer’s transaction and the customer agrees to receive the notice at a later time.

(2) Examples of exceptions.
(a) Not at customer’s election. Establishing a customer relationship is not at the customer’s election if a licensee acquires or is assigned a customer’s policy from another financial institution or residual market mechanism and the customer does not have a choice about the licensee’s acquisition or assignment.

(b) Substantial delay of customer’s transaction. Providing notice not later than when a licensee establishes a customer relationship would substantially delay the customer’s transaction when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service.

(c) No substantial delay of customer’s transaction. Providing notice not later than when a licensee establishes a customer relationship would not substantially delay the customer’s transaction when the relationship is initiated in person at the licensee’s office or through other means by which the customer may view the notice, such as on a web site.

F. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 10. If the licensee uses a short-form initial notice for non-customers according to Section 7D, the licensee may deliver its privacy notice according to Section 7D(3).

WHO RECEIVES THE PRIVACY NOTICE:

- Individuals who purchase insurance products that are primarily for personal or family use.

CONSUMERS WHO ARE NOT CUSTOMERS

The privacy notice must be given to consumers (e.g. applicants that have not been issued a policy) if their non-public personal information is shared beyond the business exceptions allowed by law. If the company does not share information beyond the exceptions, the institution need not give consumers a Privacy Statement. You should make it a practice not to share non-public personal information beyond the business exceptions allowed by law.

Before you share NPI with nonaffiliated third parties outside of the exceptions described within, 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.
SECTION 6. ANNUAL PRIVACY NOTICE TO CUSTOMERS REQUIRED

A. (1) General rule. A licensee shall provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of twelve (12) consecutive months during which that relationship exists. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the customer on a consistent basis.

(2) Example. A licensee provides a notice annually if it defines the twelve consecutive-month period as a calendar year and provides the annual notice to the customer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a customer opens an account on any day of year 1, the licensee shall provide an annual notice to that customer by December 31 of year 2.

B. (1) Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship.

(2) Examples.

(a) A licensee no longer has a continuing relationship with an individual if the individual no longer is a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee.

(b) A licensee no longer has a continuing relationship with an individual if the individual’s policy is lapsed, expired or otherwise inactive or dormant under the licensee’s business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.

(c) For the purposes of this regulation, a licensee no longer has a continuing relationship with an individual if the individual’s last known address according to the licensee’s records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

(d) A licensee no longer has a continuing relationship with a customer in the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the licensee has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.

D. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 10.
The Privacy Notice must be provided to all customers (e.g. policyowners) annually. 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.

**The Contents of the Privacy Notice**

**SECTION 7. INFORMATION TO BE INCLUDED IN PRIVACY NOTICES**

A. General rule. The initial, annual and revised privacy notices that a licensee provides under Sections 5, 6 and 9 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its privacy notice:

1. The categories of nonpublic personal financial information that the licensee collects;

2. The categories of nonpublic personal financial information that the licensee discloses;

3. The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 15 and 16;

4. The categories of nonpublic personal financial information about the licensee’s former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee’s former customers, other than those parties to whom the licensee discloses information under Sections 15 and 16;

5. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 14 (and no other exception in Sections 15 and 16 applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;

6. An explanation of the consumer’s right under Section 11A to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

7. Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

8. The licensee’s policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

9. Any disclosure that the licensee makes under Subsection B of this section.
B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 15 and 16, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

C. Examples.

(1) Categories of nonpublic personal financial information that the licensee collects. A licensee satisfies the requirement to categorize the nonpublic personal financial information it collects if the licensee categorizes it according to the source of the information, as applicable:

(a) Information from the consumer;

(b) Information about the consumer's transactions with the licensee or its affiliates;

(c) Information about the consumer's transactions with nonaffiliated third parties; and

(d) Information from a consumer reporting agency.

(2) Categories of nonpublic personal financial information a licensee discloses.

(a) A licensee satisfies the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in Paragraph (1), as applicable, and provides a few examples to illustrate the types of information in each category. These might include:

(i) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;

(ii) Transaction information, such as information about balances, payment history and parties to the transaction; and

(iii) Information from consumer reports, such as a consumer’s creditworthiness and credit history.

(b) A licensee does not adequately categorize the information that it discloses if the licensee uses only general terms, such as transaction information about the consumer.

(c) If a licensee reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.

(3) Categories of affiliates and nonaffiliated third parties to whom the licensee discloses.

(a) A licensee satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the licensee discloses nonpublic personal financial information about consumers if the licensee identifies the types of businesses in which they engage.
(b) Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.

(c) A licensee also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal financial information about consumers using more detailed categories.

(4) Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in Section 14 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Subsection A(5) of this section if it:

(a) Lists the categories of nonpublic personal financial information it discloses, using the same categories and examples the licensee used to meet the requirements of Subsection A(2) of this section, as applicable; and

(b) States whether the third party is:

(i) A service provider that performs marketing services on the licensee’s behalf or on behalf of the licensee and another financial institution; or

(ii) A financial institution with whom the licensee has a joint marketing agreement.

(5) Simplified notices. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 15 and 16, the licensee may simply state that fact, in addition to the information it shall provide under Subsections A(1), A(8), A(9), and Subsection B of this section.

(6) Confidentiality and security. A licensee describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information if it does both of the following:

(a) Describes in general terms who is authorized to have access to the information; and

(b) States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee’s policy. The licensee is not required to describe technical information about the safeguards it uses.

D. Short-form initial notice with opt out notice for non-customers.

(1) A licensee may satisfy the initial notice requirements in Sections 5A(2) and 8C for a consumer who is not a customer by providing a short-form initial notice at the same time as the licensee delivers an opt out notice as required in Section 8.

(2) A short-form initial notice shall:

(a) Be clear and conspicuous;
(b) State that the licensee’s privacy notice is available upon request; and

(c) Explain a reasonable means by which the consumer may obtain that notice.

(3) The licensee shall deliver its short-form initial notice according to Section 10. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the licensee’s short-form notice requests the licensee’s privacy notice, the licensee shall deliver its privacy notice according to Section 10.

(4) Examples of obtaining privacy notice. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:

(a) Provides a toll-free telephone number that the consumer may call to request the notice; or

(b) For a consumer who conducts business in person at the licensee’s office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.

E. Future disclosures. The licensee’s notice may include:

(1) Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal financial information.

F. Sample clauses. Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this regulation.

The notice must accurately describe how the entity collects, discloses, and protects NPI about consumers and customers, including former customers. The notice must include, where it applicable, the following information:

The initial, annual, and revised notices include, as applicable:

- **Categories of information an entity collects** (all entities). **Categories of information collected.** Nonpublic personal information obtained from an application or a third party such as a consumer reporting agency.

- **Categories of information an entity may disclose** (all entities, except an entity that does not intend to make any disclosures or only makes disclosures under the exceptions may simply state that). **Categories of information disclosed.** Information from an application, such as name, address, and phone number; Social Security number; account information; and account balances.
- **Categories of affiliates and nonaffiliates to whom an entity discloses nonpublic personal information** (all entities sharing nonpublic personal information with an affiliate or with a nonaffiliated third party). **Categories of affiliates and nonaffiliated third parties to whom the information is disclosed.** 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.

- **Information sharing practices about former customers** (all entities). **Categories of information disclosed and to whom under the joint marketing/service provider exception** in section 313.13 of the Privacy Rule.

- **Categories of information disclosed under the service provider/joint marketing exception** (only those entities relying on this exception).

- **If 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, a statement that the disclosures are made "as permitted by law." **If 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.

- **Consumer's right to opt out** (only those entities that disclose outside of exceptions)

- **Disclosures made under the Fair Credit Reporting Act** (only those entities providing the FCRA opt out notice). **Any disclosures required by the Fair Credit Reporting Act.**

- **Disclosures about confidentiality and security of information** (all entities). **Policies and practices with respect to protecting the confidentiality and security of NPI.**
RIGHT TO OPT-OUT OF INFORMATION
DISCLOSURES TO NON-AFFILIATED THIRD
PARTIES

Under the first requirement of Title V of GLB, if NPPI is shared with any non-affiliated third parties that do not fall under one of the business exceptions, allow consumers and customers the right to opt-out of (to prevent) such disclosures. If these types of disclosures are not made, the offer to Opt-out is not required.

The GLB Act gives consumers the right to "opt-out" of allowing the institution to send non-public personal information to nonaffiliated third parties. Even if the consumer does not opt-out, third parties may not re-disclose this information.

Opt-outs are also not required for institutions that want to share information with affiliates — companies that are closely related through ownership by a parent company.

FORM OF NOTICE AND OPT OUT METHODS

SECTION 8. FORM OF OPT OUT NOTICE TO CONSUMERS AND OPT OUT METHODS

A. (1) Form of opt out notice. If a licensee is required to provide an optout notice under Section 11A, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that section. The notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal financial information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt out right.

(2) Examples.

(a) Adequate opt out notice. A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal financial information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in Section 7A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.
(b) Reasonable opt out means. A licensee provides a reasonable means to exercise an opt out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;

(ii) Includes a reply form together with the opt out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee’s web site, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) Unreasonable opt out means. A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) Specific opt out means. A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. Same form as initial notice permitted. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

C. Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee’s opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in Paragraph (5) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.
(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt out direction.

(5) Example. If John and Mary are both named policyholders on a homeowner’s insurance policy issued by a licensee and the licensee sends policy statements to John’s address, the licensee may do any of the following, but it shall explain in its opt out notice which opt out policy the licensee will follow:

(a) Send a single opt out notice to John’s address, but the licensee shall accept an opt out direction from either John or Mary.

(b) Treat an opt out direction by either John or Mary as applying to the entire policy. If the licensee does so and John opts out, the licensee may not require Mary to opt out as well before implementing John’s opt out direction.

(c) Permit John and Mary to make different opt out directions. If the licensee does so:

(i) It shall permit John and Mary to opt out for each other;

(ii) If both opt out, the licensee shall permit both of them to notify it in a single response (such as on a form or through a telephone call); and

(iii) If John opts out and Mary does not, the licensee may only disclose nonpublic personal financial information about Mary, but not about John and not about John and Mary jointly.

E. Time to comply with opt out. A licensee shall comply with a consumer’s opt out direction as soon as reasonably practicable after the licensee receives it.

F. Continuing right to opt out. A consumer may exercise the right to opt out at any time.

G. Duration of consumer’s opt out direction.

(1) A consumer’s direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

(2) When a customer relationship terminates, the customer’s opt out direction continues to apply to the nonpublic personal financial information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.

H. Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 10.

If you share NPI with nonaffiliated third parties outside of the exceptions described, 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.

If an entity intends to share nonpublic personal information outside the exceptions, it must also:

• Provide consumers with a **reasonable opportunity to opt out.** Give consumers at least **30 days** to respond to the opt out notice when the entity delivers the notice by mail or electronically

• **Comply** with a consumer’s opt out direction **as soon as reasonably practicable** when the direction is received after the initial opt out period elapses

• **Comply** with the opt out direction until revoked in writing by the consumer

Entities generally may not, directly or through an affiliate, disclose a consumer’s nonpublic personal information to any nonaffiliated third party unless the consumer is given a reasonable opportunity to direct that such information not be disclosed, (to opt out). Before an entity may disclose nonpublic personal information about a consumer to a nonaffiliated third party, the entity must provide the consumer with an initial privacy notice and an opt-out notice (which may be included in the privacy notice). The GLBA contains a number of specific exceptions to these opt-out requirements, which will be discussed below. However, to ensure that entities can continue to disclose information to nonaffiliated third parties to conduct routine business. These exceptions include, for instance, the disclosure of information by entities to third parties who are providing services to the entity or to their customers as the entity’s agent.

**OPT-OUT NOTICES**

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 NPI can be disclosed to 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.

While the GLB Act does not require an opt-out notice to be provided if NPI is disclosed only to affiliates, an obligation to provide an opt-out notice may exist under the Fair Credit Reporting Act if certain information is shared with affiliates. That opt-out notice must be included in the GLB privacy notice.

An **opt-out notice** is adequate if it:

• Identifies all the categories of nonpublic personal information the entity intends to disclose to nonaffiliated third parties
- States the consumer can opt out of the disclosure
- Provides a reasonable method for the consumer to opt out, such as a toll-free telephone number

The table below summarizes the rule's requirements for delivering an opt out notice.

<table>
<thead>
<tr>
<th>Type of notice</th>
<th>Who gets it</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt out notice</td>
<td>• customers and consumers who are not customers</td>
<td>• before the bank shares nonpublic personal information about the customer or consumer (and the information sharing is not permissible under the privacy rule opt out exceptions)</td>
</tr>
</tbody>
</table>

**EXERCISING THE OPT-OUT RIGHT**

Consumers and customers must be given a "reasonable opportunity" to exercise their right to opt out, for example, 30 days, after the initial notice either on- or off-line, before their information may be shared with nonaffiliated third parties outside the exceptions. For an isolated consumer transaction, like buying a money order, entities may require 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 an opt-out direction is received from existing consumers or customers, it must be complied with as soon as reasonably possible.

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 are requiring an opt-out notice, the customer must make a new opt-out direction that will apply only to the new relationship.

**DEVELOP OPT- OUT PROCEDURES**

All entities sharing nonpublic personal information outside of the exceptions will need to develop procedures for consumers to exercise an opt out, as well as procedures for processing and complying with opt out directions. The opt out procedures should include:

- Tracking the initial opt out opportunity (e.g., the first 30 days after the initial notice is delivered)
- Recording opt outs received from consumers
- Maintaining the opt out mechanism(s), such as a toll-free telephone number, electronic mail, or an opt out form with boxes to check
- Complying with opt out directions received after the initial opt out opportunity elapses
RESPOND TO PUBLIC INQUIRIES

Customer service representatives and other employees should be prepared to answer questions from consumers about the new privacy notices. Depending on the number of employees answering consumer phone calls, it may be a good idea to provide scripts to help employees respond to questions from the public. In addition, it may be helpful to have extra copies of the privacy notice readily available for mailing or handing out to consumers.

REVISED PRIVACY NOTICES

SECTION 9. REVISED PRIVACY NOTICES

A. General rule. Except as otherwise authorized in this regulation, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 5, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 14, 15 and 16, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal financial information to any nonaffiliated third party;

(b) Discloses nonpublic personal financial information to a new category of nonaffiliated third party; or

(c) Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.

(2) A revised notice is not required if the licensee discloses nonpublic personal financial information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

C. Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 10.
A revised notice may be required when an entity changes its information sharing practices.

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

Delivery of the Privacy Notice

SECTION 10. DELIVERY

A. How to provide notices. A licensee shall provide any notices that this regulation requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

B. (1) Examples of reasonable expectation of actual notice. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not obtain an insurance product or service from the licensee electronically.

C. Annual notices only. A licensee may reasonably expect that a customer will receive actual notice of the licensee’s annual privacy notice if:

(1) The customer uses the licensee’s web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or
(2) The customer has requested that the licensee refrain from sending any information regarding the customer relationship, and the licensee’s current privacy notice remains available to the customer upon request.

D. Oral description of notice insufficient. A licensee may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.

E. Retention or accessibility of notices for customers.

(1) For customers only, a licensee shall provide the initial notice required by Section 5A(1), the annual notice required by Section 6A, and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) Examples of retention or accessibility. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:

(a) Hand-delivers a printed copy of the notice to the customer;

(b) Mails a printed copy of the notice to the last known address of the customer; or

(c) Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.

F. Joint notice with other financial institutions. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

G. Joint relationships. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.

Identify consumers and customers who must receive the initial and opt out notices. It is important to identify all groups of existing customers, consumers, and former customers who must get the initial privacy notice and opt out notification. Some entities may need to coordinate several databases and a variety of departments to identify everyone who must receive a notice.

**Opt out notices for joint account holders:** The privacy rule allows entities to provide a **single** privacy and opt out notice when two or more consumers **jointly** obtain a financial product or service. However, any of the joint consumers may exercise the right to opt out. The opt out notice provided to joint account holders must explain how the entity will treat an opt out direction by a joint consumer and must give one joint consumer the ability to opt out on behalf of all the joint consumers.

**Establish timeframes for mailing or otherwise delivering notices.** Remember:
o All existing entity customers must receive an initial privacy notice no later than July 1, 2001.

o Existing entity customers, consumers who are not customers, and former entity customers have the right to opt out if the entity is sharing nonpublic personal information about them with nonaffiliated third parties outside the exceptions.

o Information sharing subject to opt out cannot continue after July 1, 2001, until the initial and opt out notices are delivered and a reasonable opt out period has elapsed. Therefore, entities that intend to share nonpublic personal information outside the exceptions after July 1, 2001 should deliver notices well before July 1.

The GLB Act requires institutions to annually disclose their privacy policies to consumers. This disclosure must be prominent and must be made to all customers either when the customer begins his or her relationship with the institution or on an annual basis to existing customers.

The disclosure must also contain the institution's policy regarding the categories of non-public personal information it collects, its disclosure policy of non-public personal information to third parties and affiliates, and the categories of entities that receive the information.

The initial, annual, revised, and opt out notices may be delivered in writing or, if the consumer agrees, electronically. An oral description of the notice is not sufficient. Notices given orally or posted in your office(s) don't comply with the rule.

The privacy notice must be given to individual customers or consumers by mail or in-person delivery; it may not be posted on a wall. Reasonable ways to deliver a notice may depend on the type of business the institution is in an online entity may post its notice on its website and require online consumers to acknowledge receipt as a necessary part of a transaction.

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

- It can be sent in writing (e.g. hand delivered, mailed) or if agreed upon by the consumer/customer sent electronically
- It can be posted on a web site if the consumer/customer must access the page as a necessary step to obtain service.
- Posting the notice in an office or providing the statement verbally does not comply with the law.

<table>
<thead>
<tr>
<th>SUMMARY OF NOTICE REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of</td>
</tr>
</tbody>
</table>

© Copyright Sandi Kruise Insurance Training, 2004 all rights reserved
<table>
<thead>
<tr>
<th>Notice</th>
<th>Notice</th>
<th>Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Customers</td>
<td>Not later than when you establish the customer relationship, unless it would substantially delay the transaction and the customer agrees</td>
</tr>
<tr>
<td></td>
<td>Consumers who are not customers (including former customers)</td>
<td>Before you disclose their NPI to a nonaffiliated third party outside of certain exceptions</td>
</tr>
<tr>
<td>Annual</td>
<td>Customers</td>
<td>Delivery on a consistent basis at least once in any period of 12 consecutive months for the duration of the customer relationship</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)</td>
</tr>
</tbody>
</table>

**STATE REQUIREMENTS:**

- The requirement for when the privacy statement must be delivered, who receives it, and what it must contain need to be viewed on a state by state basis. Some states have adopted the legislation that has additional requirements regarding privacy.

- The 1982 Privacy Act requires that all applicants, as consumers and all customers have the right to access and request corrections to their personal information recorded by the company.

- The states in the Privacy Notice that have adopted this legislation are shown at the end of the Privacy Notice under the State Specific Requirements.
ARTICLE III. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

LIMITS ON DISCLOSURES

SECTION 11. LIMITS ON DISCLOSURE OF NONPUBLIC PERSONAL FINANCIAL INFORMATION TO NONAFFILIATED THIRD PARTIES

A. (1) Conditions for disclosure. Except as otherwise authorized in this regulation, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:

(a) The licensee has provided to the consumer an initial notice as required under Section 5;

(b) The licensee has provided to the consumer an opt out notice as required in Section 8;

(c) The licensee has given the consumer a reasonable opportunity, before it discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(d) The consumer does not opt out.

(2) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 14, 15 and 16.

(3) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:

(a) By mail. The licensee mails the notices required in Paragraph (1) of this subsection to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within thirty (30) days from the date the licensee mailed the notices.

(b) By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in Paragraph (1) of this subsection electronically, and the licensee allows the customer to opt out by any reasonable means within thirty (30) days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(c) Isolated transaction with consumer. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Paragraph (1) of this
subsection at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

B. Application of opt out to all consumers and all nonpublic personal financial information.

(1) A licensee shall comply with this section, regardless of whether the licensee and the consumer have established a customer relationship.

(2) Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.

C. Partial opt out. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

RESTRICTIONS ON REUSE AND REDISCLOSURE IF NPI IS RECEIVED UNDER THE SECTION 14 OR 15 EXCEPTIONS.

If NPI is received from a nonaffiliated financial institution ("originating financial institution") under the section 14 or 15 exceptions. In these situations, they 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. They may also disclose the information to their affiliates, who are limited in their reuse and redisclosure of the information in the same way as they are, and to affiliates of the originating financial institution.

LIMITS ON REUSE AND REDISCLOSURE OF NPI

SECTION 12. LIMITS ON REDISCLOSURE AND REUSE OF NONPUBLIC PERSONAL FINANCIAL INFORMATION

A. (1) Information the licensee receives under an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 15 or 16 of this regulation, the licensee’s disclosure and use of that information is limited as follows:

(a) The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;

(b) The licensee may disclose the information to its affiliates, but the licensee’s affiliates may, in turn, disclose and use the information only to the extent that the licensee may disclose and use the information; and
(c) The licensee may disclose and use the information pursuant to an exception in Sections 15 or 16 of this regulation, in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

(2) Example. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention, or in response to a properly authorized subpoena. The licensee may not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.

B. (1) Information a licensee receives outside of an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in Sections 15 or 16 of this regulation, the licensee may disclose the information only:

(a) To the affiliates of the financial institution from which the licensee received the information;

(b) To its affiliates, but its affiliates may, in turn, disclose the information only to the extent that the licensee may disclose the information; and

(c) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which the licensee received the information.

(2) Example. If a licensee obtains a customer list from a nonaffiliated financial institution outside of the exceptions in Sections 15 or 16:

(a) The licensee may use that list for its own purposes; and

(b) The licensee may disclose that list to another nonaffiliated third party only if the financial institution from which the licensee purchased the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee received the list, as limited by the opt out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in Sections 15 or 16, such as to the licensee's attorneys or accountants.

C. Information a licensee discloses under an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in Sections 15 or 16 of this regulation, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to the licensee’s affiliates;

(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and

(3) The third party may disclose and use the information pursuant to an exception in Sections 15 or 16 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. Information a licensee discloses outside of an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party other than under an exception in Sections 15 or 16 of this regulation, the third party may disclose the information only:
(1) To the licensee’s affiliates;

(2) To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

The privacy rule limits reuse and redisclosure of nonpublic personal information received from a nonaffiliated financial institution or disclosed to a nonaffiliated third party. The specific limitations depend on whether the information was received pursuant to or outside of the notice and opt out exceptions.

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

Even if the business is not a financial institution that has consumers or customers, the Privacy Rule may limit use of NPI. The ability to reuse and redisclose the information may be restricted if NPI is received from a nonaffiliated financial institution. It depends on why it was received.

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

Alternatively, they may receive NPI from a nonaffiliated financial institution outside the section 14 or 15 exceptions. For example, they purchase a financial institution's customer list in order to market their 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, entities may use the information internally for their own purposes. However, they may only redisclose the information consistent with the privacy policy of the originating financial institution. In other words, they 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," they 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, they cannot because that type of company is not covered by the privacy policy.

Entities may also disclose the information to their affiliates, whose redisclosure is limited in the same way, and to affiliates of the originating financial institution.

Under the Rules of Reuse, it is critical that all third parties understand the requirement under the privacy laws that affect how the third party may use the NPI that is shared with them. When
assessing a third party, particularly government and law enforcement agencies, it is important to understand how the information will be used and the level of security that will be used to protect the information.

Entities should create a privacy addendum to be applied to all third party contracts where customer information is regularly shared, to assure third parties understand the Rules of Reuse and their responsibility to protect the consumer or customer data received.

These Rules of Reuse apply to all third parties of a financial institution, which includes independent agents.

**DISCLOSURE OF ACCOUNT NUMBERS IS PROHIBITED**

**SECTION 13. LIMITS ON SHARING ACCOUNT NUMBER INFORMATION FOR MARKETING PURPOSES**

A. General prohibition on disclosure of account numbers. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer’s policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee’s service provider solely in order to perform marketing for the licensee’s own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee’s own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

C. Examples.

(1) Policy number. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a means to decode the number or code.

(2) Policy or transaction account. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A policy or transaction account does not include an account to which third parties cannot initiate charges.

The privacy rule prohibits an entity from disclosing an account number or access code for credit card, deposit, or transaction accounts to any nonaffiliated third party for use in marketing. The rule contains two narrow exceptions to this general prohibition. An entity may share account numbers in conjunction with marketing its own products as long as the service provider is not
authorized to directly initiate charges to the accounts. An entity may also disclose account numbers to a participant in a private label or affinity credit card program when the participants are identified to the customer. An account number does not include a number or code in encrypted form as long as the entity does not also provide a means to decode the number.

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 his or 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 an account number is disclosed to an agent or service provider just to market 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, the customer's consent to disclose his or her account number for marketing purposes may not be obtained.

Under the fourth basic requirement of Title V of GLB, a financial institution may not share a customer's or consumer's policy/contract number with any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail.

It is best to take a position not to share such information with any third parties (affiliated or non-affiliated) for marketing purposes.

The GLBA also provides that an entity generally may not disclose an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail, or other marketing through electronic mail to the consumer. The statute also limits the redisclosure or reuse of information obtained from other nonaffiliated financial institutions.
ARTICLE IV. EXCEPTIONS TO LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

General Exceptions:

The general business exceptions allow the sharing of non-public personal information (NPPI) for conducting business activities related to insurance.

Some examples of the general exceptions are:

- Sharing activities necessary to protect the confidentiality or security of an institution's records.
- Sharing activities necessary to protect or prevent actual or potential fraud or unauthorized transactions.
- Sharing with a consumer reporting agency in accordance with the federal Fair Credit Reporting Act.
- Compliance with federal, state or local laws, rules and other applicable legal requirements (e.g. Anti-Money Laundering requirements).

Exceptions to the Notice and Opt-Out Requirements

A consumer cannot opt out of all information sharing. First, the privacy rule does not govern information sharing among affiliated parties. Second, the rule contains exceptions to allow transfers of nonpublic personal information to unaffiliated parties to process and service a consumer's transaction, and to facilitate other normal business transactions. For example, consumers cannot opt out when nonpublic personal information is shared with a nonaffiliated third party to:

- Market the entity's own financial products or services
- Market financial products or services offered by the entity and another financial institution (joint marketing)
- Process and service transactions the consumer requests or authorizes
- Protect against potential fraud or unauthorized transactions
- Respond to judicial process
- Comply with federal, state, or local legal requirements

Applying exceptions
An entity may have to satisfy disclosure and other requirements to make the rule's opt out exceptions applicable. For example, the joint marketing exception requires a contractual agreement between two nonaffiliated financial institutions to:

a) Jointly offer, endorse, or sponsor the financial product or service, and

b) Limit further use or disclosure of the consumer information transferred

In addition, the entity must include a separate statement in the privacy notice disclosing the joint marketing agreement.

A number of exceptions apply 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 information is shared only under these sets of exceptions, there is no need to give consumers a privacy notice, but entities will need to give 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.

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

SECTION 14. EXCEPTION TO OPT OUT REQUIREMENTS FOR DISCLOSURE OF NONPUBLIC PERSONAL FINANCIAL INFORMATION FOR SERVICE PROVIDERS AND JOINT MARKETING

A. General rule.

(1) The opt out requirements in Sections 8 and 11 do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party to perform services for the licensee or functions on the licensee’s behalf, if the licensee:

(a) Provides the initial notice in accordance with Section 5; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 15 or 16 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal financial information under this section to a financial institution with which the licensee performs joint marketing, the licensee’s contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal financial information except as necessary to carry out the joint marketing or under an exception in Sections 15 or 16 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee’s own

© Copyright Sandi Kruise Insurance Training, 2004 all rights reserved
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.

Another exception can be found in section 313.13 ("section 13 exception") of the Privacy Rule. If customer and consumer information is shared under this exception, a privacy notice describing this disclosure must be provided. However, 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 do not fall within the section 14 exceptions. For example, if a nonaffiliated third party is hired to provide services in connection with marketing products or to market financial products jointly for one or more financial institutions, or to do a general analysis of customer transactions, disclosure of NPI for these purposes does not fall under the section 14 exceptions. Therefore, the section 13 exception can be used 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 a written contract has been entered with one or more financial institutions regarding the joint offering, endorsement, or sponsorship of a financial product or service. This does not apply to any kind of individual joint marketing, but only joint marketing involving financial institutions and only the marketing of financial products or services.

There are exceptions, however, to this opt-out rule, for good reason. This provision does not apply to the sharing of information with third parties to process statements or service customer accounts. Opt-out is also unnecessary when information is transferred to complete transactions authorized by the customer, when disclosing customer information to a credit bureau, complying with a regulatory investigation by state or federal authorities, or to protect against fraud.

The Privacy Addendum

Under the third basic requirement in Title V of GLB, you must enter into a privacy agreement with non-affiliated third parties that share NPPI under the processing and servicing exceptions previously discussed.

To take advantage of the section 13 exception, a contract must be entered with those nonaffiliated third parties with whom NPI is shared. 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.

### SECTION 15. EXCEPTIONS TO NOTICE AND OPT OUT REQUIREMENTS FOR DISCLOSURE OF NONPUBLIC PERSONAL FINANCIAL INFORMATION FOR PROCESSING AND SERVICING TRANSACTIONS

A. Exceptions for processing transactions at consumer’s request. The requirements for initial notice in Section 5A(2), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply if the licensee discloses nonpublic personal financial information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

1. Servicing or processing an insurance product or service that a consumer requests or authorizes;
2. Maintaining or servicing the consumer’s account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;
3. A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or
4. Reinsurance or stop loss or excess loss insurance.

B. “Necessary to effect, administer or enforce a transaction” means that the disclosure is:

1. Required, or is one of the lawful or appropriate methods, to enforce the licensee’s rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or
2. Required, or is a usual, appropriate or acceptable method:
   a. To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer’s account in the ordinary course of providing the insurance product or service;
   b. To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;
   c. To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer’s agent or broker;
   d. To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;
(e) To underwrite insurance at the consumer’s request or for any of the following purposes as they relate to a consumer’s insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

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 records; 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.

Business Exceptions

GLB provides for a number of business exceptions under which financial institutions may legally share non-public personal information (NPPI) with non-affiliated third parties.

The exceptions applicable fall under the following two categories:

- Processing and Servicing
- General Exceptions

**PROCESSING AND SERVICING**

This business exception allows the sharing of non-public personal information (NPPI) where it is required, or is one of the lawful or appropriate methods of carrying out a financial transaction, related to a product or service requested by the customer.

Some examples of processing and servicing exceptions are:

- To underwrite insurance at the consumer's or customer's request or for any of the following purposes: account administration, reporting, investigating or preventing fraud or material misrepresentation, participating in research projects or as otherwise required or specifically permitted by federal or state law.
• To administer or service benefits or claims relating to the transaction, product, or service.

• Processing premium payments or the transfer of receivables.

• The placement of or processing of reinsurance.

SECTION 16. OTHER EXCEPTIONS TO NOTICE AND OPT OUT REQUIREMENTS FOR DISCLOSURE OF NONPUBLIC PERSONAL FINANCIAL INFORMATION

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 5A(2), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply when a licensee discloses nonpublic personal financial information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee’s records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee’s compliance with industry standards, and the licensee’s attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;
(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal financial information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities;

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers’ compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 8F.

Drafting Note: Because the notice requirements of this regulation could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this regulation.
ARTICLE V. RULES FOR HEALTH INFORMATION

SECTION 17. WHEN AUTHORIZATION REQUIRED FOR DISCLOSURE OF NONPUBLIC PERSONAL HEALTH INFORMATION

A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration; claims adjustment and management; fraud investigation; underwriting; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

AUTHORIZATIONS

SECTION 18. AUTHORIZATIONS

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article V shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;
(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

B. An authorization for the purposes of this Article V shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article V at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

AUTHORIZATION REQUEST DELIVERY

SECTION 19. AUTHORIZATION REQUEST DELIVERY

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 10, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 17A.

RELATIONSHIP TO FEDERAL RULES

SECTION 20. RELATIONSHIP TO FEDERAL RULES

Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the “federal rule”), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.

Drafting Note: The drafters note that the effective date of this regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late
2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this article as of the date the licensee comes into compliance with the HHS regulation.

RELATIONSHIP TO STATE LAW

SECTION 21. RELATIONSHIP TO STATE LAWS

Nothing in this article shall preempt or supercede existing state law related to medical records, health or insurance information privacy.
ADDITIONAL PROVISIONS

ARTICLE VI. ADDITIONAL PROVISIONS

PROTECTION OF FCRA

SECTION 22. PROTECTION OF FAIR CREDIT REPORTING ACT

Nothing in this regulation shall be construed to modify, limit or supersede the operation of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be drawn on the basis of the provisions of this regulation regarding whether information is transaction or experience information under Section 603 of that Act.

NONDISCRIMINATION

SECTION 23. NONDISCRIMINATION

A. A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this regulation.

B. A licensee shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this regulation.

VIOLATION

SECTION 24. VIOLATION

Drafting Note: Cite state unfair trade practices act or other applicable state law.

SERVABILITY
SECTION 25. SEVERABILITY

If any section or portion of a section of this regulation or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation or the applicability of the provision to other persons or circumstances shall not be affected.

EFFECTIVE DATE

SECTION 26. EFFECTIVE DATE

A. Effective date. This regulation is effective November 13, 2000. In order to provide sufficient time for licensees to establish policies and systems to comply with the requirements of this regulation, the commissioner has extended the time for compliance with this regulation until July 1, 2001.

B. (1) Notice requirement for consumers who are the licensee’s customers on the compliance date. By July 1, 2001, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee’s customers on July 1, 2001.

(2) Example. A licensee provides an initial notice to consumers who are its customers on July 1, 2001, if, by that date, the licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee’s existing customers.

C. Two-year grandfathering of service agreements. Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee’s behalf satisfies the provisions of Section 14A(1)(b) of this regulation, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before July 1, 2000.
VIOLATING THE LAW

Enforcement

The FTC, the federal entities, other federal regulatory authorities, 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.

As with the basic requirements of the privacy laws themselves, the actual penalties for violating the privacy laws vary by state. Also, there are generally three categories of potential resolution for a violation:

- Fines
- Unfair Trade Practices Act
- Class Action Lawsuit

FINES

- In a number of states, violations of the state's privacy laws are punishable by fines levied against the company. The fines may be on a "per occurrence" basis, meaning that a specific amount is applied to each individual instance of non-compliance, or the state may levy a fine based on the severity of the violation. In either case, the fines apply even if the act was not intentional. In most states, the total amount of the fines is capped at a specific dollar amount.

UNFAIR TRADE PRACTICES ACT:

- In many states violations of the privacy law are punishable under the state's Unfair Trade Practices Act. In many cases, this results in fines and, depending upon the seriousness or extent of the violation, the state Attorney General or Insurance Commissioner may file suit on behalf of the individuals harmed by the company's actions. The monetary damages under the fines and lawsuit could be substantial. Even more significant is the damage to a company's reputation and the level of customer trust.

CLASS ACTION LAWSUIT

- In some states, the ability to introduce a private suit or class action lawsuit may fall under the Unfair Trade Practices Act. Thus, in those states, the government and private
citizens may sue the insurer under the Unfair Trade Practices Act. Also, state privacy laws may specifically allow class action lawsuits thereby opening a company to significant damages both monetarily and to their reputation. Again, individuals involved in the class action lawsuits must show they have been damaged by the company's negligence.

CIVIL AND CRIMINAL PENALTIES FOR VIOLATION OF THE ADMINISTRATIVE SIMPLIFICATION PORTION OF HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

(NOTE: PENALTIES ARE IDENTIFIED IN HIPAA STATUTE ONLY)

Congress, in order to assure accountability of those who had access to personal health information (PHI) required the imposition of civil monetary penalties for any entity or person that uses PHI improperly. The improper uses and associate penalties are described below:

CIVIL PENALTIES

<table>
<thead>
<tr>
<th>Monetary Penalty</th>
<th>Term of Imprisonment</th>
<th>Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>$100</td>
<td>N/A</td>
<td>Single violation of a provision (can be multiple violations with penalty of $100 each as long as each violation is for a different provision)</td>
</tr>
<tr>
<td>$25,000</td>
<td>N/A</td>
<td>Multiple violations of an identical requirement or prohibition made during a calendar year</td>
</tr>
</tbody>
</table>

CRIMINAL PENALTIES

<table>
<thead>
<tr>
<th>Monetary Penalty</th>
<th>Term of Imprisonment</th>
<th>Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to $50,000</td>
<td>Up to one year</td>
<td>Wrongful disclosure of individually identifiable health information</td>
</tr>
<tr>
<td>Up to $100,000</td>
<td>Up to five years</td>
<td>Wrongful disclosure of individually identifiable health information committed under false pretenses</td>
</tr>
<tr>
<td>Up to $250,000</td>
<td>Up to 10 years</td>
<td>Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm</td>
</tr>
</tbody>
</table>
Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

**A-1—CATEGORIES OF INFORMATION A LICENSEE COLLECTS (ALL INSTITUTIONS)**

A licensee may use this clause, as applicable, to meet the requirement of Section 7A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

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

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates or others; and
- Information we receive from a consumer reporting agency.

**A-2—CATEGORIES OF INFORMATION A LICENSEE DISCLOSURES (INSTITUTIONS THAT DISCLOSE OUTSIDE OF THE EXCEPTIONS)**

A licensee may use one of these clauses, as applicable, to meet the requirement of Section 7A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 14, 15 and 16.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as “your name, address, social security number, assets, income, and beneficiaries”;
- Information about your transactions with us, our affiliates or others, such as “your policy coverage, premiums, and payment history”; and
- Information we receive from a consumer reporting agency, such as “your creditworthiness and credit history”.
Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as “above” or “below”].

A-3—CATEGORIES OF INFORMATION A LICENSEE DISCLOSES AND PARTIES TO WHOM THE LICENSEE DISCLOSES (INSTITUTIONS THAT DO NOT DISCLOSE OUTSIDE OF THE EXCEPTIONS)

A licensee may use this clause, as applicable, to meet the requirements of Sections 7A(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 15 and 16.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4—CATEGORIES OF PARTIES TO WHOM A LICENSEE DISCLOSES (INSTITUTIONS THAT DISCLOSE OUTSIDE OF THE EXCEPTIONS)

A licensee may use this clause, as applicable, to meet the requirement of Section 7A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 14, 15 and 16, as well as when permitted by the exceptions in Sections 15 and 16.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [provide illustrative examples, such as “life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents”];
- Non-financial companies, such as [provide illustrative examples, such as “retailers, direct marketers, airlines, and publishers”]; and
- Others, such as [provide illustrative examples, such as “non-profit organizations”].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5—SERVICE PROVIDER/JOINT MARKETING EXCEPTION

A licensee may use one of these clauses, as applicable, to meet the requirements of Section 7A(5) related to the exception for service providers and joint marketers in Section 14. If a licensee discloses nonpublic personal information under this exception, the licensee shall
describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

**Sample Clause A-5, Alternative 1:**

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, income, and beneficiaries”];
- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your policy coverage, premium, and payment history”]; and
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your creditworthiness and credit history”].

**Sample Clause A-5, Alternative 2:**

We may disclose all of the information we collect, as described [describe location in the notice, such as “above” or “below”] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

**A-6—Explaination of Opt Out Right (Institutions that Disclose Outside of the Exceptions)**

A licensee may use this clause, as applicable, to meet the requirement of Section 7A(6) to provide an explanation of the consumer’s right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 14, 15 and 16.

**Sample Clause A-6:**

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as “call the following toll-free number: (insert number)].

**A-7—Confidentiality and Security (All Institutions)**

A licensee may use this clause, as applicable, to meet the requirement of Section 7A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

**Sample Clause A-7:**

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as “those employees who need to know that information 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.
Title V of the Gramm-Leach-Bliley Act (GLBA) calls on state insurance regulators to promulgate rules enforcing the privacy protections embedded in the Act. All states have taken action to comply with that mandate.1

A key element of GLBA’s privacy protections – and by far the most visible to consumers - is the privacy notice. The purpose of the privacy notice is to explain the licensee’s privacy policies to its customers, and to other consumers whose nonpublic personal information may be subject to disclosure to third parties. The notices are intended to assist consumers in making informed decisions about how to exercise their legal and contractual rights with regard to their personal information, and in comparing licensees’ information practices when shopping for insurance and other financial services.

Privacy notices must contain specific information about a licensee’s privacy policies, such as the types of protected information the insurer collects, the types of protected information the insurer discloses, and the categories of entities to which the insurer discloses such information.

Financial institutions, including licensees, were first required to send privacy notices to customers by July 1, 2001. After that date, financial institutions are required to provide notices annually to customers, and to certain other consumers as well. Since the first privacy notices were sent in mid-2001, there has been a great deal of discussion and debate over the effectiveness of the notices. Did the notices really do what Congress and the regulators intended? Did they explain the financial institution’s privacy policy in a way that clearly informs customers as to what information is protected and when/where/how such protected information is disclosed?

Many notices have been described as confusing, complicated and overly legalistic. That is not to say that financial institutions are not in compliance with GLBA and applicable regulations, or that they did not make great efforts to draft notices to be clear and understandable. The problem is that it is a very difficult task.

Throughout its discussions, the NAIC Privacy Notice Subgroup (the Subgroup) focused on finding ways to help licensees craft GLBA privacy notices that are simpler, shorter, and more understandable to insurance consumers. Avenues for improving privacy notices are described in this Report. The Report focuses on general themes – such as formatting text, and the placement and merging of the various required elements of the notice – and offers specific suggestions for improving the terminology used in 1 As of February 2003, 36 states and the District of Columbia have enacted laws and/or regulations based on the NAIC Privacy of Consumer Financial and Health Information Model Regulation. Thirteen states have retained the Insurance Information and Privacy Protection Model Act, which was adopted by the NAIC in the early 1980s, and one state has regulations pending. 2
placement and order of items

1. Placement and Ordering of Items in the Notice

Anecdotal evidence suggests that the itemization of the required topics in most licensees' privacy notices is similar and generally follows the same order, which is the order found in Appendix A of the NAIC Privacy of Consumer Financial and Health Information Model Regulation (the Model Regulation) and tracks the order in which those topics are addressed in Section 7 of the Model Regulation, which prescribes the required minimum content of privacy notices.2

The Privacy Notice Subgroup believes that the order in which the sample clauses are presented in Appendix A is not necessarily the optimal placement of information in a licensee's privacy notice. Indeed, any strict requirement as to the placement of information in a nonstandardized notice could impede the notice's effectiveness.

Mandating a “one size fits all” order of presentation could cause the notice to be “front loaded” with a great deal of information that may not be the most important information for that licensee’s customers. The Subgroup encourages licensees to determine the most effective order for the material in their privacy notices, based on the importance of the information to their customers. Licensees should consider placing the more meaningful information and information about any action items (such as opt out instructions) up front.

combining items in the notice

2. Combining Items in the Notice

The Subgroup discussed the possibility of combining the various required sections of the notice. The Subgroup agreed that combining sections would have the potential to reduce redundancy and length, and improve clarity. The general consensus of the Subgroup was that when many customers received the initial notice, they did not bother to read the notice because it was long
and difficult to read. Therefore, the notice was not serving the purpose for which it was intended: to notify the customers of the licensee’s privacy policy. For that reason, the Subgroup suggests that companies consider 2 Appendix A, based on its counterpart in the federal interagency rules, lists sample clauses that can be used in privacy notices. The model regulation does not require that notices disclose information in a particular order. The samples are there merely to illustrate acceptable language. This report in no way alters the validity of the sample clauses in Appendix A. 3

combining sections where possible and taking other steps to create a shorter notice without sacrificing the content of the notice.

One combination of sections could be the blending of the “Categories of information the licensee collects” with the “Categories of information a licensee discloses.” If a former customer’s information is handled in the same way that information about current customers is handled, the “Categories of nonpublic personal financial information about the licensee’s former customers that the licensee discloses” can be combined, as well. An example of such a combination is:

We collect and may share information about you, some of which is not publicly available. We may share this information now or in the future. We do this to enable us to serve you and to help us to identify you as our customer or our former customer, to process your policy and requests quickly, to pay your claim or tell you about products or services we believe you may want and use.

- **Information from you** – When submitting your application or requesting an insurance quote, you may give us information such as your name, address, and Social Security number.

- **Information about your transactions** – We may keep information about your transactions with us or our family of companies, for example, the products you purchase from us, the amount you paid for the insurance, your account balances, or payment history.

- **Information from outside our family of companies** – We also may collect other information. This may include information from consumer reporting agencies such as your credit history, credit scores, driving record or employment.

If applicable, companies can also consider listing the categories of nonaffiliated third parties to which they disclose information outside the exceptions in the same section of their notice. An example of this combination could be:

We may share your name, address, telephone number and demographics, now or in the future, with companies outside of our family of companies such as banks, motor vehicle manufacturers or dealers, parts suppliers, health clubs, travel agencies, car rental agencies, hotels, airlines, or publishers. These companies may offer other financial or non-financial products and services, such as travel programs, magazine subscriptions, dental or legal services, exercise programs, diet programs, credit cards, or mortgages. You will have the opportunity to request that we do not share this information.3

3 As discussed in section 1, placement of items can be a useful tool to make notices simpler and more effective. A licensee that discloses information to non-affiliated third parties outside
the exceptions (or offers the right to opt out of disclosures to affiliates) may wish to follow this item with a discussion of opt out rights.

If the licensee does not disclose outside of the exceptions, that licensee could combine the “Categories of nonpublic personal financial information that the licensee discloses” with the “Disclosure that the licensee makes under the exceptions” (as opposed to exercising the licensee’s prerogative “to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.”) An example of the combination could be:

We may occasionally convey the information we collect – such as your name, address, e-mail, product information or transaction information – to companies outside of our family of companies in order to:

- Perform services for us, such as printing payment coupons, preparing or mailing account statements, processing customer transactions or software programming, or helping us market our own products.

- Offer you financial products that we currently don’t offer, like credit cards or specialized programs.

By combining sections, the licensee may be able to provide a shorter notice in length, while not sacrificing the content of the notice. The Subgroup believes this will result in clearer, more concise notices that are fully read by customers.

Terms

3. Use of “Terms of Art”

The Subgroup recognized that the use of “terms of art” in notices could be confusing to customers who are not familiar with insurance and privacy terminology. In order to help consumers better understand the terms in the notices, licensees may wish to define the terms or use common words with the same meanings. A non-exhaustive list of words and phrases synonymous with selected privacy notice terms are listed below. Note that the many words synonymous with “share” illustrate the vast array of meanings this term can possess. As they draft their notices, licensees should be mindful of the requirement in the Model Regulation (and in the various laws and regulations tracking the Model Regulation) that notices be clear and conspicuous, and may refer for guidance to the examples in the definition of “clear and conspicuous.” Licensees should be as precise as possible when using synonyms to avoid further confusing or inadvertently misleading consumers.

OPT-OUT

- Stop
- Exercising the right to confidentiality/privacy
- As a customer you have the right, with limited exceptions, to choose whether your information remains confidential or is given out to other companies /firms /enterprises /businesses.
• Prohibit
• With certain exceptions, you may choose not to let companies:
  o Reveal information
  o Give away…
  o Disclose…
  o Exchange…
  o Offer…
• You may choose to limit information given to others
• You have the choice of allowing our company to offer your information to other companies for their use/viewing
• You can choose to keep information:
  o Confidential
  o Private
  o Protected

DISCLOSE
• Share
• Give
• Distribute
• Make known
• Release
• Display
• Make public

AFFILIATES
• Companies within our “family” of companies
• Partners/copartners
• Sister companies
• Companies related to our company
• Companies under common ownership

NON-AFFILIATED THIRD PARTIES
• Companies outside our “family” of companies
• Not associated with our company
• Not related to our company
• Not legally linked with/to our company

NON-PUBLIC PERSONAL FINANCIAL INFORMATION
• Information that is not publicly available
• Protected information
• Private information
Companies should consider whether the simple phrase “customer information” could substitute for the more technical “non-public personal information” or any of the synonyms above. This would likely depend in large part on how they handle disclosures of information.

**PUBLICLY AVAILABLE INFORMATION**

- Information that is unprotected
- Open records information
- Commonly available information
- Information freely available through the media
- Information available through public records
- Information in the public domain

**SHARE:**

- Sell
- Provide
- Trade
- Furnish
- Exchange
- Give
- Offer
- Make available to
- Deliver
- Market
- Supply

Explaining Disclosures

4. Explaining Disclosures “Permitted by Law”

The Model Regulation permits licensees to simply state, “we disclose information as permitted by law” to explain all disclosures made pursuant to sections 15 and 16. These exceptions are generally for legal and “doing business” purposes.

Anecdotal evidence suggests that some consumers are suspicious when they see “permitted by law,” thinking their information will be widely distributed no matter what the rest of the privacy notice says. The Subgroup believes a better approach for consumers and licensees alike is to more fully explain these disclosures with examples or a more complete description. A fuller explanation gives consumers – who are not likely to know what is “permitted by law” – a better understanding of how their information is disclosed, and may promote better customer relations.

In addition to explaining the legal and business exceptions that are “permitted by law,” the Subgroup believes that it would be helpful to consumers for licensees to explain that they are also permitted to share information freely with their affiliates. Although neither GLBA nor the model regulation mandates any disclosure by a licensee regarding the licensee’s right to share
information with its affiliates, the Subgroup believes it would be consumer-friendly to include a clear discussion of this point. This would also offer licensees the opportunity to inform their consumers if they voluntarily limit their power to share information with some or all affiliates.

The following provisions are examples of language that could be incorporated into notices to improve the description of disclosures “permitted by law.”

- **We may also share personal information about you with companies or other organizations outside of the [INSURER] family as required by or permitted by law. For example, we may share personal information to:**
  - Protect against fraud;
  - Respond to a subpoena; or
  - Service your account.

- **We Share Information for Legal and Routine Business Reasons.** We may disclose information we have about you as permitted by law. For example, we may share information with government regulators and law enforcement agencies. We may provide information to protect against fraud. We may report account activity to credit bureaus. We may share information with your consent. We may give account information such as [list examples] to service providers who work for us.

- **Other Circumstances Where We May Share Your Information:** We may share customer information in other circumstances. Some examples are:
  - When you specifically request it or give us permission to do so;
  - When we are required by law. For example, we may be required to share information with insurance regulators;
  - When we share information with consumer reporting agencies;
  - When we suspect fraud or criminal activity;
  - When we receive a subpoena;
  - When we are ordered by a court to do so; and
  - When we sell a particular line of business or function.

- **In certain circumstances, [INSURER] may share your customer information with trusted service providers that need access to your information to provide operational or other support services.** To ensure the confidentiality and security of your information, service providers must agree to safeguard your information in strict compliance with our policy. Additionally, when you apply for a [INSURER] policy, [INSURER] may share information about your application with credit bureaus. We also may provide information to regulatory authorities and law enforcement officials in accordance with applicable law or when we otherwise believe in good faith that the law requires it. In the event of a sale of all or part of one of our businesses, we may share customer information related to that business as part of the transaction.

- **We may share information as permitted by law.** For example, providing information to industry regulators, to law enforcement agencies, for fraud prevention, to credit bureaus and to third parties that assist us in processing the transactions you authorize and in mailing statements to you.

- **Sometimes we may share your information with other companies affiliated with us or our parent company [NAME], particularly if they support our efforts to provide you with services and product information.**
- Sometimes we may also share your information with a company or business not officially connected to us but who may do work on our behalf.
- And sometimes we may disclose information about you to an insurance regulatory authority, a government agency or a law enforcement official.
- Various industry and professional organizations may also ask us for customer information in order to conduct research studies. These studies are purely scientific in nature and never identify individuals.
- Finally, if we do provide your information to any party outside our company we require them to abide by the same privacy standards as indicated here.

### Introduction / Preamble

#### 5. Brief Introduction/Notice Preamble

Anecdotal evidence suggests that many consumers do not know why they are receiving privacy notices. Therefore, the Subgroup believes it may be helpful for a licensee to explain to consumers why it is sending the notice, even though neither GLBA nor the NAIC model requires such an explanation. If the explanation were a brief introduction to the privacy notice, it could also offer licensees the opportunity to highlight key issues in the notice, for example items in the notice that address marketing disclosures, opt out rights, etc.

There are a number of benefits that flow from use of an introductory statement. First, it is necessarily generic, so it can be used uniformly by insurance licensees without regard to their unique information handling practices and without changing individual GLBA privacy notices. Second, it is adaptable, so licensees can incorporate the statement into existing privacy notices relatively easily. Third, and most importantly, it is informative, allowing insurance consumers to see at a glance the privacy protections afforded by GLBA and directing those consumers to the more detailed description of a licensee’s information handling practices outlined in the individual privacy notices. The brief introduction could contain statements about the following basic GLBA provisions (as augmented by the Model Regulation):

- **Privacy policy.** Licensees must have privacy policies describing their personal information collection practices, and the extent to which they share that information with third parties for purposes other than normal business operations.

- **Privacy notice.** Licensees must provide privacy notices to customers, reflecting their privacy policies, when the relationship is established and annually thereafter. A privacy notice must also be provided to applicants and certain other noncustomers when their personal information is shared with a third party for marketing purposes, or other purposes for which disclosure without consent is not expressly permitted or required by law.

- **Marketing “opt-out.”** Licensees must provide their customers, applicants, and other consumers with the opportunity to “opt-out” from having their personal financial information shared with third parties for marketing purposes. The only exceptions are for financial information shared with a corporate affiliate, with the licensee’s own service providers or under a joint marketing agreement with another financial institution.
• **Medical information authorization.** Licensees may not share personal health information for marketing purposes with anyone, including affiliates, unless the licensee has received affirmative authorization to do so.

• **Business operations and legal disclosures.** Licensees may share personal information for non-marketing business operations and for legal purposes without consent.

• **Affiliates.** Except for health information, the restrictions on sharing personal information with third parties do not apply if the third party is under common ownership with the licensee.

---

### Formatting Notices

#### 6. Formatting Notices

Dynamic formatting is another way to make notices more inviting and easier to read, while still taking care to include all the required elements in the notice. Incorporating the themes and suggested language changes outlined in this Report with improved visual appeal may also increase the effectiveness of privacy notices.

Again, it may be helpful to refer to the examples in the definition of “clear and conspicuous” in the Model Regulation and in the various laws and regulations tracking the Model Regulation. In addition, a licensee may wish to consider the following to increase readability:

- Use of readable typefaces, including size (12-point type suggested) and fonts (easy to read fonts like Times and Arial; consider different fonts for text and headings);
- Use of **bold** and *italics* to make words and phrases stand out;
- DON’T OVERUSE ALL CAPITAL LETTERS BECAUSE IT’S DIFFICULT TO READ;
- Use of informative headings (“Our Security Practices Protect Your Information,” “We Don’t Share Your Information with Companies Outside Our Corporate Family,” “We Share Your Information for Legal and Routine Business Reasons”);
- Use of bulleted or numbered lists; and
- Use of short sentences and short paragraphs.

---

### Conclusion

#### 7. Conclusion

Drafting GLBA privacy notices is a difficult process, made more difficult by the need to comply with specific legal requirements and the desire to draft a readable, consumer-friendly notice that effectively presents the licensee’s privacy policy. The Subgroup recognizes the difficulty of this task. In consultation with industry and consumer representatives, the Subgroup has identified methods that may improve notices so that they are both GLBA-compliant and consumer-friendly.
Re-ordering and combining required elements;
Explaining phrases and terms of art;
Adding a short preamble describing why the notice is being sent; and
Dynamic formatting.

Licensees are encouraged to regularly review their notices with these suggestions in mind, remembering that the goal is to make the notices simple, readable and effective.

Develop privacy policies and notices

Use this opportunity to evaluate and establish institutional privacy objectives, and communicate to potential customers and consumers the entity’s customer service philosophy.

Create a comprehensive inventory of information collection and information sharing practices at the entity. The inventory will help ensure practices are properly disclosed in the entity’s privacy notices.

For every department, review:

- All applications and forms used to collect information about consumers
- Marketing practices
- Vendor contracts
- Electronic entity and Internet activities
- Fee income accounts
- Record retention policies

Affiliates: If an entity has any affiliates, the inventory should include information-sharing practices with affiliates. Although the privacy rule does not place any restrictions on information sharing with affiliates, it does require disclosure of these practices in the initial and annual notices. Furthermore, the privacy rule requires the initial and annual notices to include applicable Fair Credit Reporting Act affiliate information sharing opt out notices. Assess current information collection and information sharing practices in light of the privacy rule obligations and the entity’s objectives. Determine which practices should continue after July 1, 2001. Consider:

- Whether any current practices would be prohibited under the rule
- Which practices must be disclosed in the privacy notices and whether opt out rights apply
Whether account numbers are shared only as permitted by the rule

Whether information received from other financial institutions is shared only as permitted by the rule's reuse and redisclosure limitations

Whether to adopt voluntary privacy standards developed by relevant trade associations. Those standards could be good indicators of industry norms and consumer expectations

Drafting privacy notices

Draft privacy notice(s). Create a list of information collection and information sharing practices that must be disclosed to consumers. This list can help you categorize practices per the rule requirements and decide how to structure notices. The privacy rule provides a variety of disclosure options. For example, entities may develop:

- One initial privacy notice that covers all the information sharing practices of the entity

- An assortment of initial notices for different customer relationships or different types of financial products or services. One initial notice that covers the practices of the entity along with one or more of its affiliates. Likewise, the opt out notice may be structured in a variety of ways.

Sample clauses provided in Appendix A in the rule. Entities may use the sample clauses to the extent they accurately reflect the entity's practices.

Most likely, the initial and annual privacy notices will be identical. If required, the opt out notice may be combined with the initial and annual notices.

Writing Effective Financial Privacy Notices

Since 2001, the Gramm-Leach-Bliley (GLB) Act has required financial institutions to provide notices that explain their privacy practices and their customers’ rights. Many notices satisfy the basic legal requirement to explain obligations and rights accurately, but they fall far short when it comes to providing explanations that are meaningful to the reader.

An effective privacy notice includes:

- A customer-based process that invites and uses consumer feedback

- Plain language that enables a short, simple, easy-to-read message

- Graphics that make a notice attractive and inviting

Legal experts should review the drafts to make sure the notices are accurate and satisfy the requirements of the law.

To refine messages, solicit feedback from customers who have received a notice. Many customers may not be familiar with privacy issues in general, and their privacy rights in particular. Many of them may not have read a privacy notice before.
Meaningful communication can enhance customer confidence and trust – and that the GLB notice requirement can offer an opportunity to make that happen. A user-friendly notice reflects how much your company values its customers.

**PLAIN LANGUAGE**

A notice should start with a description of the purpose of the notice and the questions it will answer. This tells readers why to read the notice.

Use informative headings to preview what follows, and where appropriate, let customers know whether there’s an action step.

**Notice language should be:**

- Concise - simple and straightforward, not jargon.
- Direct - using the word "you" to engage reader.
- Affirmative - telling customers what is, rather than what isn't; what they should do, rather than what they shouldn't do.
- Active rather than passive.
- Respectful.

If technical terms must be used, help your reader understand them:

- Define the term in a text box close to its use.
- Include a glossary in the notice.
- On a website, hyperlink the term to a definition or use a simpler term or phrase in the text and link to the technical term.

Company contact information should be clear and conspicuously displayed.

**GRAPHICS**

Design the notice with attractive and pleasing styles and formats. Consider:

- The typeface
  - 12 point preferable; at a minimum, 10-point type
  - Serif fonts for paper
  - Sans serif fonts for headings and Web
  - Use upper and lower case
- Bold, italics or underlining for emphasis
- Headings
- Bullets or numbers
- Color for interest
- Graphics, symbols and text boxes
- Indents to show subcategories of information or examples
- Limit the length of the document as well as individual paragraphs and sentences.

Appropriate use of white space between text and margins
COMPLYING WITH THE SAFEGUARDS RULE

Security and Confidentiality Guidelines for Customer Data

Many financial institutions collect personal information from their customers, such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.

The final requirement of GLB pertains to security and confidentiality guidelines to protect the confidentiality of the customer information within a financial institution's control.

As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) has issued the Safeguards Rule. This Rule requires financial institutions under FTC jurisdiction to secure customer records and information.

The GLB Act requires financial institution regulators to establish standards to ensure the confidentiality and security of consumer records, protect against threats to the security of those records, and protect against unauthorized access to those records that could result in substantial harm or inconvenience to the consumer.

The GLB Act's sweeping definition of "financial institution" means any regulated financial company or business that engages in financial activities. It includes banks, bank holding companies, securities firms, insurance companies, insurance agencies, thrifts, credit unions, mortgage brokers, finance companies, and check cashers.

In 2002, the NAIC adopted a Model Security Regulation to assist states in establishing standards for development and implementation of safeguards by insurers to protect customer information. Several individual states have adopted this Security Regulation. Firms should base responses to the issue of security by applying the NAIC Model Security Regulation to its electronic and hardcopy security practices.

SAFEGUARDING NPI

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

WHO MUST COMPLY

The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers, including Insurance Companies and Agents. The Safeguards Rule also applies to financial companies, like credit reporting agencies and ATM operators, that receive information from other financial institutions about their customers. In addition to developing their own safeguards, financial institutions are responsible
for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

**The Safeguard Rule**

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). Consult the FTC's website at [www.ftc.gov/privacy/glbact/index.html](http://www.ftc.gov/privacy/glbact/index.html) for more information about this rule and further guidance for small businesses in implementing the Safeguards Rule requirements.

The Safeguards Rule is posted at [www.ftc.gov/privacy/glbact](http://www.ftc.gov/privacy/glbact).

Adequately securing customer information is not only the law, it is also good business practice. When customers know that we care about the security of their personal information, it increases their level of confidence in the institution. Poorly-managed customer data can lead to identity theft. Identity theft occurs when someone steals a consumer's personal identifying information to open new charge accounts, order merchandise or borrow money.

**Copies** of the Federal Register notice and a business alert, "Safeguarding Customers Personal Information: A Requirement for Financial Institutions," are available from the FTC's Web site at [http://www.ftc.gov](http://www.ftc.gov) and also from the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. 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 any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at [http://www.ftc.gov](http://www.ftc.gov). The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
Standards for Safeguarding Customer Information; Final Rule

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") is issuing a final Safeguards Rule, as required by section 501(b) of the Gramm-Leach-Bliley Act ("G–L–B Act" or "Act"), to establish standards relating to administrative, technical and physical information safeguards for financial institutions subject to the Commission’s jurisdiction.

As required by section 501(b), the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

EFFECTIVE DATE: This rule is effective on May 23, 2003.

FOR FURTHER INFORMATION CONTACT:

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

A. Background
B. Overview of Comments Received
C. Section-by-Section Analysis
D. Paperwork Reduction Act
E. Regulatory Flexibility Act

Section A. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Pub. L. 106–102) into law. The purpose of the Act was to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. The Act permits banks to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities.

Subtitle A of Title V of the Act, captioned "Disclosure of Nonpublic Personal Information," limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose certain privacy policies and practices with respect to its information sharing with both affiliates and nonaffiliated third parties. On May 12, 2000, the Commission issued a final rule, Privacy of
Consumer Financial Information, 16 CFR part 313, which implemented Subtitle A as it relates to these requirements (hereinafter “Privacy Rule”). The Privacy Rule took effect on November 13, 2000, and full compliance was required on or before July 1, 2001.

Subtitle A of Title V also requires the Commission and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information. See 15 U.S.C. 6801(b), 6805(b)(2). As described in the Act, the objectives of these standards are to: (1) Ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. See 15 U.S.C. 6801(b)(1)–(3).

The Act does not require all of the agencies to coordinate in developing their safeguards standards, and does not impose a deadline to establish them.

Although the Act permits most of the agencies to develop their safeguards standards by issuing guidelines, it requires the SEC and the Commission to proceed by rule.

On September 7, 2000, the Commission issued for publication in the Federal Register an Advanced Notice of Proposed Rulemaking (“the ANPR”) on the scope and potential requirements of a Safeguards Rule for the financial institutions subject to its jurisdiction. The Commission received thirty comments in response to the ANPR.

Based on these comments, as well as the safeguards standards already issued by the other GLB agencies, the Commission issued a Notice of Proposed Rulemaking respecting Standards for Safeguarding Customer Information (“the proposal” or “the Proposed Rule”) on August 7, 2001. In response to the proposal, the Commission received forty-four comments from a variety of interested parties. The Commission now issues a final rule governing the safeguarding of customer records and information for the financial institutions subject to its jurisdiction (“Safeguards Rule”).

Like the proposal, the Final Rule requires each financial institution to develop a written information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. As described below, each information security program must include certain basic elements to ensure that it addresses the relevant aspects of a financial institution’s operations and that it keeps pace with developments that may have a material impact on its safeguards.

In developing the Final Rule, the Commission carefully weighed the comments, including concerns expressed about the ability of smaller and less sophisticated financial institutions to meet the Rule’s requirements. It also sought to ensure that the Rule mirrored the requirements of the guidelines already established by the NCUA and the other banking agencies (collectively, “the Banking Agency Guidelines”), with adjustments as needed to clarify the Rule’s scope and accommodate the diverse range of entities covered by the Commission’s Rule. The Commission believes that the Final Rule strikes an appropriate balance between allowing flexibility to financial institutions and establishing standards for safeguarding customer information that are consistent with the Act’s goals. As described below, the Commission will issue educational materials in connection with the Rule in order to assist businesses—and in particular, small entities—to comply with its requirements without imposing undue burdens.
Section C. Section-by-Section Analysis

Consistent with the proposal, the Safeguards Rule will be part 314 of 16 CFR, to be entitled “Standards for Safeguarding Customer Information.” This Part will follow the Privacy Rule, which is contained in part 313 of 16 CFR. The following is a section-by-section analysis of the Final Rule.

Section D. Paperwork Reduction Act

The Paperwork Reduction Act ("PRA"), 44 U.S.C. Chapter 35, requires federal agencies to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons. 44 U.S.C. 3502(3)(a)(i). Under the PRA, a rule creates a “collection of information” where ten or more persons are asked to report, provide, disclose, or record information” in response to “identical questions.” See 44 U.S.C. 3502(3)(A). Applying these standards, the Rule does not constitute a “collection of information.” The Rule calls upon affected financial institutions to develop or strengthen their information security programs in order to provide reasonable safeguards. Under the Rule, each financial institution’s safeguards will vary according to its size and complexity, the nature and scope of its activities, and the sensitivity of the information involved. For example, a financial institution with numerous employees would develop and implement employee training and management procedures beyond those that would be appropriate or reasonable for a sole proprietorship, such as an individual tax preparer or mortgage broker. Similarly, a financial institution that shares customer information with numerous affiliates would need to take steps to ensure that such information remains protected, while a financial institution with no affiliates would not need to address this issue. Thus, although each financial institution must summarize its compliance efforts in one or more written documents, the discretionary balancing of factors and circumstances that the Rule allows—including the myriad operational differences among businesses that it contemplated—does not require entities to answer “identical questions,” and therefore does not trigger the PRA’s requirements. See “The Paperwork Reduction Act of 1995: Implementing Guidance for OMB Review of Agency Information Collection,” Office of Information and Regulatory Affairs, OMB (August 16, 1999), at 20–21.

Section E. Regulatory Flexibility Act

In its ANPR, the Commission stated its belief that, under the Regulatory Flexibility Act ("RFA"), 5 U.S.C. 604(a), it was not required to issue an Initial Regulatory Flexibility Analysis ("IRFA") because the Commission did not expect that the Proposed Rule would have a significant economic impact on a substantial number of small entities within the meaning of the Act. See 66 FR at 41167. The Commission nonetheless issued an IRFA with the Proposed Rule in order to inquire into the possible impact of the Proposed Rule on small entities, and to provide information to small businesses, as well as other businesses, on how to implement the Rule. Id. Although the Commission specifically sought comment on the costs to small entities of complying with the Rule, no commenters provided specific cost information. Some commenters generally praised the proposal’s flexibility 82 or noted that given its flexible standards, it was appropriate for the Rule to apply equally to businesses of all sizes.83 However, other commenters suggested that small entities may be disproportionately burdened by the Rule because they lack expertise (relative to larger entities) in developing, implementing and maintaining the required safeguards.84 In light of these comments, the Commission has carefully considered whether to certify that the Rule will not have a significant impact on a substantial number of small entities.
The Commission continues to believe that the Rule’s impact will not be substantial in the case of most small entities. However, the Commission cannot quantify the impact the Rule will have on such entities. Therefore, in the interest of thoroughness, the Commission has prepared the following Final Regulatory Flexibility Analysis (“FRFA”) with this Final Rule. 5 U.S.C. 605.

Under the Act, the Commission has jurisdiction over “any other financial institution or other person that is not subject to the jurisdiction of any agency or authority.” 15 U.S.C. Section 6805(7). Thus, the Commission does not have jurisdiction over any financial institution that is subject to another Agency’s authority by the Act, including national banks, bank holding companies and savings associations the deposits of which are insured by the FDIC. See id. at Section 6805(a)(1)–(6).

Final Rule

For the reasons set forth in the preamble, the Federal Trade Commission amends 16 FR chapter I, subchapter C, by adding a new part 314 to read as follows:

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

The Federal Trade Commission has issued a final rule governing the safeguarding of customer records and information for the financial institutions subject to its jurisdiction. The Rule implements the safeguards provisions of the Gramm-Leach-Bliley Act (GLB Act), which require the Commission and certain other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for customer information. The objectives of these standards are to: ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer.

In drafting the Final Rule, the Commission sought to ensure that the Rule’s requirements would accommodate the diverse range of financial institutions that are subject to its jurisdiction. Thus, the Final Rule requires each of these financial institutions to implement an information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.
314.1 Purpose and scope.
314.2 Definitions.
314.3 Standards for safeguarding customer information.
314.4 Elements.
314.5 Effective date.

Many financial institutions’ transactions with customers involve the collection of personal information: names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley (GLB) Act, a federal law, requires that financial institutions take steps to ensure the security and confidentiality of this kind of customer data.

As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued a rule to require the financial institutions under its jurisdiction to safeguard customer records and information.

The Safeguards Rule applies to individuals or organizations that are significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers.

**Section 314.1: Purpose and Scope**

§ 314.1 Purpose and scope.

(a) **Purpose.** This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) **Scope.** This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (“FTC” or “Commission”) has jurisdiction. This part refers to such entities as “you.” This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

Paragraph 314.1(a) states that the Rule is intended to establish standards for financial institutions to develop, implement and maintain administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. This paragraph also states the statutory authority for the proposed Rule.

**Section 314.2: Definitions**

§ 314.2 Definitions.
(a) **In general.** Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission’s rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) **Customer information** means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) **Information security program** means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) **Service provider** means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

This section defines terms used in the Safeguards Rule. As under the proposal, paragraph (a) makes clear that, unless otherwise stated, terms used in the Safeguards Rule bear the same meaning as in the Commission’s Privacy Rule. The remaining paragraphs (b)-(d) of this section define the terms “customer information,” “information security program,” and “service provider,” respectively.

### Section 314.3: Standards for Safeguarding Customer Information

§ 314.3 Standards for safeguarding customer information.

(a) **Information security program.** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) **Objectives.** The objectives of section 501(b) of the Act, and of this part, are to:

1. Insure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
Proposed paragraph (a) of this section set forth the general standard that a financial institution must meet to comply with the Rule, namely to “develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards” that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue. This standard is highly flexible, consistent with the comments, the Banking Agency Guidelines, and the Advisory Committee’s Report, which concluded that a business should develop “a program that has a continuous life cycle designed to meet the needs of a particular organization or industry.”

Section 314.4: Elements

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;
(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

According to the Safeguards Rule, financial institutions must develop a written information security plan that describes their program to protect customer information. All programs must be appropriate to the financial institution’s size and complexity, the nature and scope of its
activities, and the sensitivity of the customer information at issue. Covered financial institutions must:

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

The Rule will require financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards. As part of its program, each financial institution must:

- **Designate the employee** or employees to coordinate the safeguards;
- **Identify and assess the risks** to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- **Design a safeguards program**, and detail the plans to monitor it;
- **Select appropriate service providers** and require them (by contract) to implement the safeguards; and
- **Evaluate the program and explain adjustments** in light of changes to its business arrangements or the results of its security tests.

This section sets forth the general elements that a financial institution must include in its information security program. The elements create a framework for developing, implementing, and maintaining the required safeguards, but leave each financial institution discretion to tailor its information security program to its own circumstances.

These requirements are designed to be flexible. Each financial institution should implement safeguards appropriate to its own circumstances. For example, some financial institutions may choose to describe their safeguards programs in a single document, while others use several different documents. A company may decide to designate a single employee to coordinate safeguards or may spread this responsibility among several employees who will work together.

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

### Securing Information

Experts suggest that three areas of operation present special challenges and risks to information security: employee training and management; information systems, including network and software design, and information processing, storage, transmission and retrieval; and security management, including the prevention, detection and response to attacks, intrusions or other system failures. The Rule requires financial institutions to pay special attention to these areas.
When a firm implements safeguards, the Safeguards Rule requires it to consider all areas of its operation, including three areas that are particularly important to information security: employee management and training; information systems; and managing system failures. Firms should consider implementing the following practices in these areas.

**EMPLOYEE MANAGEMENT AND TRAINING**

The success or failure of your information security plan depends largely on the employees who implement it. You should:

- Check references prior to hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
  - Locking rooms and file cabinets where paper records are kept;
  - Using password-activated screensavers;
  - Using strong passwords (at least eight characters long);
  - Changing passwords periodically, and not posting passwords near employees' computers;
  - Encrypting sensitive customer information when it is transmitted electronically over networks or stored online;
  - Referring calls or other requests for customer information to designated individuals who have had safeguards training; and
  - Recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.
- Instruct and regularly remind all employees of your organization's policy - and the legal requirement - to keep customer information secure and confidential. Provide employees with a detailed description of the kind of customer information handled (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored
- Limit access to customer information to employees who have a business reason for seeing it. Grant access to customer information files to employees, but only to the extent they need it to do their job.
- Impose disciplinary measures for any breaches.
INFORMATION SYSTEMS

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on how to maintain security throughout the life cycle of customer information - that is, from data entry to data disposal:

• Store records in a secure area. Make sure only authorized employees have access to the area. For example:
  
  o Store paper records in a room, cabinet, or other container that is locked when unattended;
  
  o Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
  
  o Store electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area;
  
  o Don’t store sensitive customer data on a machine with an Internet connection; and
  
  o Maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.

• Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information. Specifically:
  
  • If credit card or other sensitive financial data is collected, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;
  
  • If information is collected directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail; and
  
  • If sensitive data must be transmitted by electronic mail, ensure that such messages are password protected so that only authorized employees have access.

• Dispose of customer information in a secure manner. For example:
  
  • Hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;
  
  • Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up;
• Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information;

• Effectively destroy the hardware; and

• Promptly dispose of outdated customer information.

Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. Consider supplementing all customer lists with at least one controllable entry (such as an account number or address), and monitor use of this entry to detect all unauthorized contacts or charges.

Maintain a close inventory of all computers.

MANAGING SYSTEM FAILURES

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions:

• Maintain up-to-date and appropriate programs and controls by:

  • Following a written contingency plan to address any breaches of physical, administrative or technical safeguards;
  
  • Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
  
  • Using anti-virus software that updates automatically;
  
  • Maintaining up-to-date firewalls, particularly if broadband Internet access is used or if employees are allowed to connect to the network from home or other off-site locations; and
  
  • Providing central management of security tools for employees and passing along updates about any security risks or breaches.

• Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. Back up all customer data regularly.

• Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. Use tools such as passwords, as well as personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically.

• Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.
Section 314.5: Effective Date

§ 314.5 Effective date.

(a) Each financial institution subject to the Commission’s jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002, by direction of the Commission.

Proposed section 314.5 required each financial institution covered by the Rule to implement an information security program not later than one year from the date on which a Final Rule is issued. In addition, the proposal requested comment on whether the Rule should contain a transition period to allow the continuation of existing contracts with service providers, even if the contracts would not satisfy the Rule’s requirements.

Donald S. Clark, Secretary.

[FR Doc. 02–12952 Filed 5–22–02; 8:45 am]
BILLING CODE 6750–01–P

The Commission vote to publish the Rule was 5-0. It will become effective one year from publication in the Federal Register, with additional time before compliance is required for contracts with service providers.
How This Impacts Agents

- Agents must understand the basic requirements of the Privacy Policy to conform to them in daily work.

- Agents must know the company is committed to maintaining privacy of customer information in accordance with the law.

- Agents must own responsibility for bringing Privacy questions or concerns to the Privacy Officer. In particular, promptly reporting any breaches of privacy if they occur.

- Agents need to follow the Confidentiality & Security Guidelines.

FURTHER GUIDANCE

For additional information about the GLB Act and the Privacy Rule, please visit the FTC’s GLB Act website at www.ftc.gov/privacy/glbact/index.html. Information available at that site will include written guidance, prepared by the staff of the FTC and other federal agencies enforcing the GLB Act.

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 www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357). The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
SUMMARY - Maintaining Compliance

The following activities can help an entity achieve and maintain compliance with the privacy rule.

- **Develop controls to monitor ongoing compliance.** Consider mechanisms for monitoring:
  
  - Delivery of initial and annual notices to customers
  
  - Delivery of initial notice to consumers who are not customers, if applicable
  
  - Compliance with opt out directions, if applicable
  
  - Accuracy of privacy notices, including prior approval for:
    
    - New marketing arrangements
    
    - New or renewed vendor contracts
    
    - Disclosure of account numbers
    
    - Affiliate-referral programs
    
    - Reuse of consumer information received from another financial institution

- **Train employees.** All employees should understand the entity's policies and procedures for complying with the privacy rule. Some employees will need to be able to explain the entity's privacy policies to customers and to businesses providing services to the entity.

- **Audit for compliance.** Periodic audits will help management assess risk and verify the effectiveness of the compliance program.
## STATE LEGISLATION AND REGULATIONS ON PRIVACY

### Implementation of Title V of Gramm-Leach-Bliley

#### PROGRESS ON STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

**MODEL REGULATION**

The date in parentheses is the effective date of the legislation or regulation, with the latest amendments.

<table>
<thead>
<tr>
<th>NAIC MEMBER</th>
<th>PRIVACY MODEL REG. CITATION AND STATUS</th>
<th>SAFEGUARDING MODEL CITATION AND STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>Ins. Reg. 122 requires compliance with the provisions of Title V of GLBA by all insurers, producers and other licensees of the insurance dept. Amended to adopt part of NAIC model.</td>
<td>NO ACTION TO DATE</td>
</tr>
<tr>
<td>Alaska</td>
<td>HB 184 (2001) is authority to adopt regs to protect privacy of health and financial information. Reg. tit. 3 §§ 26.605 to 26.749 pending.</td>
<td>NO ACTION TO DATE</td>
</tr>
<tr>
<td>Arizona</td>
<td>Insurance Information and Privacy Protection Model Act in place as §§ 20-2101 to 20-2120. SB 1288 (2001) amended that statute.</td>
<td>NO ACTION TO DATE</td>
</tr>
<tr>
<td>California</td>
<td>Insurance Information and Privacy Protection Model Act in place as Ins. §§ 791.01 to 791.26. SB 773 pending. AB 1775 pending (2002); reg. pending; similar to model privacy regulation (2002).</td>
<td>CAL. ADMIN. CODE tit. 10 §§ 2689.12 to 2689.20 pending (2002).</td>
</tr>
<tr>
<td>Colorado</td>
<td>Ins. Reg. 6-4-1</td>
<td>COLO. ADMIN. INS. REG. 6-4-2 (2002) (Eff. 6/1/03).</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Insurance Information and Privacy Protection Model Act in place as §§ 38a-975 to 38a-998; SB 352 (2002) authorizes regulations consistent with GLBA. Reg. 38a-8-105 to 38a-8-123 pending</td>
<td>NO ACTION TO DATE</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>Insurance Information Privacy Protection and Safeguarding Reg in place as DC code: ch. 36 of tit. 26</td>
<td></td>
</tr>
</tbody>
</table>
Florida
SB 2174 (2001) (Authority to adopt model).
Reg. 4-128.001 to 4-128.024
FLA. ADMIN. CODE §§ 4-128.030 to 4-128.035 pending (2002).

Georgia
Reg. 120-2-87 adopted 8/13/01.
NO ACTION TO DATE

Hawaii
SB 1550 (2001)
NO ACTION TO DATE

Idaho
§ 41-1334 is authority to adopt regulations consistent with title V of GLBA.
Ins. Reg. 48 (2001)
NO ACTION TO DATE

Illinois
Insurance Information and Privacy Protection Model Act in place as 215 ILCS 5/1001 to 5/1024. Reg. tit. 50 §§ 4001.10 to 4001.50 require compliance with the provisions of Title V of GLBA by insurers, producers and other licensees. Reg. tit. 50 §§ 4002.10 to 4002.240.
ILL. ADMIN. REG. tit. 50 §§ 4003.10 to 4003.110 pending (2002).

Indiana
Reg. 760:1-67 adopted as emergency regulation.
NO ACTION TO DATE

Iowa
SB 2409 (2000) requires the commissioner to adopt privacy rules concerning information held by insurer or agent consistent with GLBA. Reg. 191-90.1 to 191-90.21

Kansas
§ 40-2404 gives authority to adopt rules no more restrictive than the standards contained in regulations promulgated under Title V of Gramm-Leach-Bliley Act by federal regulatory agencies governing financial institutions. HB 2480 (2001) amends the authority to require that the commissioner adopt rules consistent with the NAIC model. Reg. 40-1-46 (financial information adopted 7/1/01; health information adopted eff. 3/1/02)
NO ACTION TO DATE

Kentucky
Reg. 806 KAR 3:210E; 806 KAR 3:220E adopted as emergency regulations.
NO ACTION TO DATE

Louisiana
Reg. 37:XIII.9901 to 37:XIII.9953 (Ins. Reg. 76)
NO ACTION TO DATE

Maine
Insurance Information and Privacy Protection Model Act in place as tit. 24-A §§ 2201 to 2220. LD 1640 (2001) gives authority to adopt regulations implementing GLBA. Effective 9/21/01. Bulletin 308 explain to insurers; brochure explains to consumers.
ME. INS. REG. ch. 980 pending (2002).

Maryland
HB 362 (2001) gives the commissioner authority to adopt a regulation consistent with the NAIC model. Reg. 31.16.08 effective 1/21/02.
NO ACTION TO DATE

Massachusetts
Insurance Information and Privacy Protection Model Act in place as 175I:1 to 175I:22. HB32, HB 229, HB 2356, HB 3036 pending.
NO ACTION TO DATE

Michigan
SB 431 (2001)
NO ACTION TO DATE
Minnesota Insurance Information and Privacy Protection Model Act in place as §§ 72A.49 to 72A.505. NO ACTION TO DATE

Mississippi SB 2207 (2001) gives the commissioner authority to adopt regulations to implement the Gramm-Leach-Bliley Act. Ins. Reg. 2000-1; Emergency Ins. Reg. 2000-2 extended the time for compliance with GLBA to 8/1/01. NO ACTION TO DATE

Missouri HB 801, SB 382 (2001) is authority to adopt regulation. Reg. tit. 20 § 100-6.100 NO ACTION TO DATE

Montana Insurance Information and Privacy Protection Model Act in place as §§ 33-19-101 to 33-19-409, amended by SB 465 (2001) to address GLBA. NO ACTION TO DATE

Nebraska LB 52 (2001) with eff. date of 7/1/01 for financial information and 1/1/03 for health information. NO ACTION TO DATE

Nevada Insurance Information and Privacy Protection Model Act in place as Reg. §§ 679B.560 to 679B.750. AB 618 (2001) is authority to adopt regulations. Regulation under development expected eff. in 2002. Hearing 6/28/02. NO ACTION TO DATE

New Hampshire Reg. 3001.01 to 3006.05 (2001) (Financial eff. 7/1/01; health eff. 12/31/01) NO ACTION TO DATE

New Jersey Insurance Information and Privacy Protection Model Act in place as §§ 17:23A-1 to 17:23A-22. NO ACTION TO DATE

New Mexico SB 352 (2001) is authority to promulgate regulations. Reg. 13.1.3.1 to 13.1.3.28 eff. 2/25/02 NO ACTION TO DATE


North Carolina Insurance Information and Privacy Protection Model Act in place as §§ 58-39-1 to 59-39-120. SB 461 amends that law to comply with GLBA. NO ACTION TO DATE

North Dakota SB 2127 (2001) gives authority to the commissioner to adopt rules regarding disclosure of non-public personal information. Reg. 45-14-01-01 to 45-14-01-22 eff. 12/1/01. NO ACTION TO DATE

Ohio Insurance Information and Privacy Protection Model Act in place as §§ 3904.1 to 3904.22. NO ACTION TO DATE

Oklahoma HB 1341 (2001) is authority to adopt regulations. Reg. 365:30-1-1 to 365:30-1-54 (Eff. 1/5/02) NO ACTION TO DATE

Pennsylvania  
Reg. 146a.1 to 146a-44 retroactively eff. to 7/1/01.  
NO ACTION TO DATE

Rhode Island  
Reg. 99 (2001) (Financial); Reg. 100 (2001) (Health)  
NO ACTION TO DATE

South Carolina  
Ins. Reg. 69-58 (Health portion eff. 1/1/03)  
NO ACTION TO DATE

South Dakota  
SB 3 (2001) is authority to adopt rules related to financial privacy.  
Reg. 20:06:45 (2001)  

Tennessee  
SB 1637 (2001)  
Reg. 0780-1-72 (2001)  
NO ACTION TO DATE

Texas  
**SB 11 and SB 712 (2001) (gives authority to adopt regulations). Duty to enforce privacy rules of GLBA. Bulletin B-0030-01 describes department plans. Reg. 28 TAC §§ 22.1 to 22.26; Reg. 28 TAC §§ 22.51 to 22.67**  
NO ACTION TO DATE

Utah  
SB 100 (2001) gives authority to adopt regulations;  
Reg. R590-206-1 to R590-206-26;  
Reg. R590-210-1 to 590-210-7 exempts manufacturer warranty and service contracts from the provisions of R590-206.  

Vermont  
**Reg. IH-2001-01**  
NO ACTION TO DATE

Virginia  
NO ACTION TO DATE

Washington  
Reg. 284-04-120 to 284-04-620 adopted with eff. date of 7/1/01  
NO ACTION TO DATE

West Virginia  
SB 507 (2001) is authority to adopt regulation.  
Reg. 114-57-1 to 114-57-22 adopted as emergency regulation  

Wisconsin  
Ins. Reg. 25.01 to 25.95  
NO ACTION TO DATE

Wyoming  
SB 60 (2001) gives authority to adopt a regulation regarding the disclosure of nonpublic personal financial and health information consistent with NAIC model. Reg. 54; financial provisions eff. 1/5/02 and health eff. 1/1/03.  
Regulation pending (2002).

---

Every effort is made to keep this information up-to-date. However, you may want to consult directly with state legislative and regulatory bodies for the most recent activity.

* Indicates that the state previously enacted legislation based on the 1982 NAIC Privacy Protection Model Act.
PRIVACY PROVISIONS OF OTHER LAWS

The statutes, however, differ in the scope of their coverage, as well as in their requirements with respect to an entity’s treatment of consumer information. As a result, what may be a permissible disclosure under one statute may be prohibited or subject to different conditions under the other statute. Because compliance with one statute will not entail compliance with the other, entities are therefore strongly advised to evaluate the requirements of both laws in connection with their disclosures of consumer information.

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 clear and conspicuous disclosures to consumers regarding sharing of certain information (such as consumer report and application information) with affiliates, they must continue to do so. The GLB Act requires these disclosures to be made as part of any privacy policy given to consumers or customers. More information about the FCRA and how it applies to information sharing practices is available at www.ftc.gov/os/statutes/fcrajump.htm.

Principal FCRA Information Sharing Provisions

The FCRA sets standards for the collection, communication, and use of information bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. The communication of this type of information may be a "consumer report" subject to the FCRA’s requirements. The definition of consumer report contains a number of exceptions, however, including exceptions that permit an entity:

- To share with any other party information solely as to the entity’s transactions or experiences with a consumer; and

- To share with entity affiliates other types of information, such as information from a credit report or from a consumer’s loan application, if it is clearly and conspicuously disclosed to the consumer that such information sharing may occur, and the consumer is given an opportunity to direct that the information not be shared, i.e., to "opt out."

Entities that share consumer report information among affiliates or with third parties under other circumstances may become consumer reporting agencies subject to the FCRA’s requirements applicable to those entities. These requirements relate to furnishing consumer reports only for permissible purposes, maintaining high standards for ensuring the accuracy of information in consumer reports, resolving customer disputes, and other matters.

As a general matter, an entity will not be subject to the FCRA’s substantial requirements that apply to consumer reporting agencies if the entity communicates only transaction or experience information to third parties or among its affiliates. Additionally, an entity will not become a consumer reporting agency if it shares with its affiliates other information that would ordinarily be considered consumer report information if it does so in accordance with the consumer opt-out process noted above. The FCRA does, however, impose a number of requirements on
persons that use consumer reports or furnish information to consumer reporting agencies, and these provisions can apply to national entities and their subsidiaries. Several of these provisions protect the privacy of consumer information, including one that requires an entity to use or obtain consumer reports only for specific permissible purposes under the statute. Another provision requires an entity that solicits consumers for offers of credit based on information in consumer reports ("prescreened offers") to provide a clear and conspicuous notice with each offer informing consumers, among other things, how they can opt out of further solicitations.

Electronic Fund Transfer Act

The EFTA and the Federal Reserve Board’s Regulation E (12 C.F.R. Part 205) require that entities make certain disclosures at the time a consumer contracts for an electronic fund transfer service or before the first electronic fund transfer is made involving the consumer’s account. For example, the financial institution must disclose the circumstances under which, in the ordinary course of business, the financial institution may provide information concerning the consumer’s account to third parties, whether or not the third party is affiliated with the entity. This disclosure must encompass any information that may be provided concerning the account (not just information relating to the electronic fund transfers themselves).

Right to Financial Privacy Act

The RFPA prohibits financial institutions from disclosing a customer’s financial records to the federal government except in limited circumstances such as pursuant to the customer’s authorization, an administrative subpoena or summons, a search warrant, a judicial subpoena, or a formal written request in connection with a legitimate law enforcement inquiry, or to a supervisory agency in connection with its supervisory, regulatory, or monetary functions.

Children’s Online Privacy Protection Act

The COPPA and the Federal Trade Commission’s implementing regulations (16 C.F.R. Part 312) generally apply to financial institutions that operate commercial web sites or online services (or portions thereof) that are directed to children, or that operate web sites or online services and knowingly collect personal information from children under the age of 13.

COPPA and the FTC’s regulations establish a number of requirements applicable to operators of covered web sites and online services, including requirements that the operator must provide online notice about its information practices with respect to children. With limited exceptions, the operator also must obtain verifiable parental consent prior to any collection, use, or disclosure of personal information from children. The operator also must provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance. Operators also are prohibited from conditioning a child’s participation in a game, the offering of a prize, or any other activity upon the child’s disclosing more personal information than is reasonably necessary to participate in such activity. Finally, operators must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.
General Laws

National entities and their subsidiaries also should be aware of other federal and state laws that may affect their practices relating to consumer financial information. For example, on the federal level, the Federal Trade Commission Act (15 U.S.C. 41 et seq.) prohibits unfair or deceptive acts or practices in or affecting commerce, and provides a basis for government enforcement actions against deception resulting from misleading statements concerning a company’s privacy practices or policies, or failures to abide by a stated policy. A number of states have enacted privacy laws that specifically relate to the disclosure of consumer financial information, as well as laws that more generally target unfair and deceptive acts and practices. The GLBA maintains that state laws that afford greater protection for consumer privacy than that provided by the GLBA are not preempted by Title V of the GLBA. The FCRA, however, provides that state laws that prohibit or impose requirements on the exchange of information among affiliates are preempted unless enacted after January 1, 2004.
L
Law .............................................. 12, 21, 79
Lawsuit ..................................................... 68
Legal ............................................ 80, 82, 84
Licensee ................................................... 21
M
Medical ..................................................... 82
Model Privacy Act ...................................... 9
Model Security Regulation ....................... 87
Money ...................................................... 56
Mortgage .................................................. 19
Multiple violations ..................................... 69
N
NAIC .......................4, 9, 74, 75, 81, 87, 106
National Association of Insurance
Commissioners ................................. 9
Nonaffiliated ................................... 9, 22, 50
Nonaffiliated third party .................... 22
Nondiscrimination .............................. 10, 66
Nonpublic personal financial information 12, 23, 24
Nonpublic personal health information ..... 25
Nonpublic personal information .... 23, 24, 38
NPI ......23, 24, 25, 33, 35, 38, 39, 43, 46, 49, 51, 53, 55, 57, 58, 87, 88
O
Offense .................................................... 69
Opt out ............................................... 47, 50
Opt out notice ............................................ 47
Opt-Out ............................................ 7, 11, 43, 44, 56, 57
Our ......................................................... 82
P
Partial ....................................................... 51
Partial opt out ........................................... 51
Partners ................................................... 78
Penalty ...................................................... 69
Personaly identifiable financial information ........................................ 23, 24, 26, 27
Plain Language ........................................ 85
Policies ..................................................... 39
Policy number ........................................ 54
Principal .................................................. 107
Privacy ....0, 4, 6, 7, 8, 9, 17, 19, 23, 30, 31, 33, 35, 39, 45, 46, 48, 49, 53, 55, 57, 58, 61, 68, 74, 75, 81, 84, 87, 89, 91, 94, 101, 106, 108
Privacy Act.......................4, 9, 49, 61, 108
Privacy Addendum ....................... 6, 58
Private ..................................................... 78
Processing and Servicing ........... 10, 59, 60
Publicly available information ........24, 27
Publicly Available Information ........28, 79
R
Reasonable basis ..................................... 27
Reasonably understandable .......... 14
Redisclosure .................................... 9, 51, 53
Retention ............................................... 47
Reuse ................................................. 9, 51, 53, 54, 102
S
Safeguards .................. 87, 88, 89, 90, 91, 93, 94, 95, 96, 97
Safeguards Rule ...87, 88, 89, 90, 91, 93, 94, 95, 96, 97
Sample clause ..................................... 38, 84
Sample clauses .............................. 38, 84
Scope ............................................. 9, 12, 93
SEC .......................................................... 90
Secure ..................................................... 98
Secure Sockets Layer .................... 98
Securities .............................................. 8, 61
Securities and Exchange Commission .8, 61
Security ............................................. 82, 87, 101
Service provider ...................... 71, 94
Service provider/joint marketing exception .................................................. 71
Severability ......................................... 10, 67
Short-form initial notice .............. 37
Single violation ............................... 69
Social Security .................. 24, 38, 76, 87, 93
State .............................................. 6, 10, 12, 22, 38, 49, 65
Substantial delay ...................... 33
T
term ......................................................... 69
Termination ........................................ 34
Termination of customer relationship .... 34
Terms of Art. .............................................. 77
Title V ....4, 5, 11, 13, 40, 55, 58, 74, 89, 90, 103, 109
Trade ...12, 61, 68, 79, 89, 92, 93, 100, 108, 109
Transaction ........................................ 36
Transfer ................................................... 4, 108
Treasury ................................................... 61
V
Vendor ..................................................... 83

W
We.........................70, 71, 72, 76, 77, 80, 82

Wrongful disclosure.................................69

Y
You .................33, 35, 39, 43, 76, 78, 94, 97
Your.....................................................80, 82