Independent Insurance Agents & Brokers of America, Inc.

# THE PRIVACY PROVISIONS OF THE GRAMM-LEACH-BLILEY ACT AND THEIR IMPACT ON INSURANCE AGENTS & BROKERS

This memorandum is not intended to provide specific advice about individual legal, business or other questions. It was prepared solely as a guide, and is not a recommendation that a particular course of action be followed. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional should be sought.

**PREPARED BY THE OFFICE OF THE GENERAL COUNSEL**

Updated as of April 2006

## I. Introduction

The Financial Modernization Act of 1999, more commonly known as the "Gramm-Leach-Bliley Act" ("GLBA") was signed by President Clinton on November 12, 1999 and greatly affects the financial services industry. The GLBA repealed the 66-year old Glass-Seagall Act which prohibited banks, securities firms and insurance companies from being affiliated. Under the GLBA, banks, securities firms and insurance companies may now be affiliated under Financial Holding Companies.

Title V of the GLBA provides certain privacy protections for consumers' nonpublic personal financial information held by financial institutions. Under Title V of the GLBA, the term "financial institutions" includes insurance agents and brokers. This memorandum will deal exclusively with Title V of the GLBA and its affect upon insurance agents and brokers.

It is important to remember that although GLBA's privacy protections are federal mandates, **their implementation vis-a-vis the insurance industry falls to the applicable state insurance authorities through the development of state laws, regulations, or both.**

The National Association of Insurance Commissioners ("NAIC") has adopted a model privacy regulation consistent with the requirements of the GLBA and the federal privacy regulations. Many states have promulgated individual state regulations identical (or nearly identical) to the NAIC model regulation.

Check with your state association to learn more about how your state is implementing the Gramm-Leach-Bliley Act for its insurance agents and brokers.

## II. Requirements For Insurance Agents & Brokers Under the GLBA

The GLBA imposes three overarching privacy obligations:

**A. Privacy Notice Disclosure Requirement.** Every insurance agency must provide all "customers" with an initial and annual notice that describes the manner in which their nonpublic personal information is collected, maintained, and disseminated. Every individual having dealings with an insurance agency is considered a "consumer", but only those consumers with a specific or ongoing relationship with the insurance agency are "customers." Only the information of individuals that is used for personal, family, or household purposes is regulated under each of these privacy regimes. Information regarding businesses is not protected in any way. [1] See Section III for a detailed discussion of the privacy disclosure requirements. See Appendix I for a Sample Privacy Policy Notice.

**B. Opt Out Notification Requirement.** Before an insurance agency may share "nonpublic personal information" about a "consumer" with a non-affiliated third party for a "non-exempted purpose," the "consumer" must be notified of the right to prohibit the sharing of such information for such a purpose (an "opt out" right).[2] States have the right to create an opt in right for consumers under state law.[3] See Section IV for a detailed discussion of the opt out requirements. See Appendix I for a Sample Opt Out Notice.

C. **Data Security and Integrity Requirement.** All agencies that collect or maintain a customer's nonpublic personal information must institute mechanisms for protecting the security and integrity of that information. See Section VI for a detailed discussion of the data security and integrity requirements.

## II. Information Protected by the GLBA

[1] This means that information gathered in connection with commercial coverages, including directors and officers insurance or keyman insurance, is not protected under the GLBA.
[2] For a discussion of exempted purposes, see Section IV D.
[3] In American Council of Life Insurers, et al. v. Vermont Department of Banking, Insurance, Securities, and Healthcare Administration, et al., Washington Superior Court No. 56-1-02, the Court upheld the state's opt-in financial privacy regulation against a challenge brought by a group of insurance companies.

The cornerstone of the GLBA privacy obligations is the protection of "nonpublic personal information." Nonpublic personal information means personally identifiable financial information that a consumer provides to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution as well as any list or grouping of consumers that is derived using any personal information not publicly available. The term does not include publicly available information. This term is expansive and includes the following examples:

- Information provided on loan, credit card, or insurance applications;
- Bank account or policy number information;
- Information from a consumer report, and
- Information collected through an Internet "cookie."

An example of a consumer list that is protected because it is developed from nonpublic personal information is a list of consumers' names and street addresses derived in whole or in part using policy information, such as a list of customers who have purchased homeowners insurance. A consumer list that does not identify a specific consumer, such as aggregate information or blind data, without names, addresses or other nonpublic personally identifying information, however, would not be subject to GLBA protections.

While these examples clarify what it means for information to be "personal," there is another component to the definition – the information must not be "publicly available" to qualify for protection. To ensure the reasonableness of a belief that information is publicly available, an agency should confirm that the information is of the type that is available to the general public, and take steps to determine if the consumer has sought to keep the information private. For example, an agency would have a reasonable basis to believe that mortgage information is publicly available if it determines that the information is of the type included on the public record where the mortgage is recorded. Likewise, an agency would have a reasonable basis to believe that an individual's phone number is publicly available if the phone number is listed.

## III. The GLBA Privacy Notice Requirement

### *A. Who Must Receive Notice?*

The GLBA notice obligation requires all insurance agencies to provide an easily understandable notice of their privacy practices to their "customers" when a "customer relationship" is established and at least annually thereafter during the continuation of the relationship.

In addition, a privacy notice must be provided to all "consumers"[4] if the agency is going to share that information obtained from a consumer with a non-affiliated entity for a non-exempted purpose.[5] If the agency does not plan to share the personal information of these "consumers" with a non-affiliated third party for a non-exempted purpose, then the agency does not owe them a privacy notice.

### B. *What Must Be Included In The Notice?*

As noted above and unlike the opt out requirement, the GLBA does not dictate the specific type of privacy policy that an agency must adopt. Instead, an agency need only disclose certain facts about its privacy policies. The disclosures must include the policies and practices of the agency with respect to disclosing nonpublic personal information to affiliates or nonaffiliated third parties including:

(1) The categories of nonpublic personal information that are collected by the agency (including the nature of the data collected and the means by which it is collected if the collection means are not obvious (such as by passive electronic monitoring)).

(2) The categories of affiliates and non-affiliated third parties to whom such disclosures are or may be made, other than those to whom information is disclosed under an exception.

(3) The agency's policies and practices with respect to sharing nonpublic personal information about former customers. If an agency's policies are the same for customers and former customers, it may use the same clauses for both.

(4) The individual's right to opt out of the disclosure of nonpublic personal information to non-affiliated third parties.

(5) Any disclosures regarding affiliate information sharing that the agency is providing under the FCRA.

---

[4] A "consumer" is defined as an individual (or the individual's legal representative) who obtains from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes.

[5] The privacy notice is provided to consumers in connection with an opt out notification. The opt out notification requirement is addressed in Section IV, below.

(6) The agency's policies and practices with respect to protecting the confidentiality, security, integrity and quality of the nonpublic personal information it collects.

These disclosures must be "clear and conspicuous," which means they must be reasonably understandable and designed to call attention to their nature and significance. A notice will likely be viewed as being reasonably understandable if it uses short and clear explanatory sentences or bullet lists in plain language. A notice calls attention to the nature and significance of the information in it through the use of headings; easy-to-read type-styles and font sizes; putting key words in boldface or italics; or using shading or sidebars to draw attention to the notice when it is presented in combination with other information.

GLBA prohibits nonpublic personal information from being shared with a nonaffiliated third party for a non-exempted purpose unless the consumer has been offered (and declined to exercise) the requisite opt out right. If an agency revises its privacy policy to permit the sharing of information with a nonaffiliated third party that was not identified as a potential recipient of the information for a purpose that was not identified, the nonpublic personal information cannot be shared with such a nonaffiliated third party until the consumer has been notified of the revised policy and been given the requisite opportunity to opt out.

### C. *When and How Should These Disclosures Be Made?*

In general, an insurance agency's privacy policy must be disclosed initially when a "customer relationship" is established and on at least an annual basis thereafter. Agencies have three options for providing notice to their customers. They may:

(1) Provide their own notice to the customer;

(2) Provide a joint notice to the customer on behalf of both the agency and a carrier; or

(3) Deliver the carrier's notice to the individual on the carrier's behalf.

Under all of these options, the initial notice can be provided when a purchased policy is delivered or when an agreement to provide other insurance services is consummated. The notice itself can be provided as part of or in conjunction with other materials that an agency delivers to customers, including with the insurance contract or in an envelope with a bill for premiums.

The annual notice to customers also may be provided in these ways. Agencies should note that the GLBA does not require them to provide the annual privacy notice to a *former customer* – an individual with whom the institution no longer has a continuing relationship. Title insurance agents and other providers of real estate settlement services whose contact with the insured is limited to the time when the policy is sold are excused from the subsequent annual notice requirement after the initial notice is provided.

Finally, agencies that sell group insurance policies should note that the provision of their privacy notice to a plan sponsor (or group or blanket insurance policyholder) satisfies their notice obligations to plan participants (or individuals covered under the policy) as long as the agencies do not disclose the participants' personal information to non-affiliated entities other than as permitted under an exception. Similarly, an agency's obligations are satisfied by providing notice to a workers compensation plan participant and refraining from disclosing any protected information about that participant's beneficiaries to non-affiliated third parties for non-exempted purposes.

## IV. The GLBA Opt Out Notice Requirement

In addition to the privacy policy disclosure notice, before disclosing nonpublic personal information about any individual to a non-affiliated third party for a non-exempted purpose, the agency must notify the consumer or customer that the information may be shared and that he or she has a right to direct the agency not to disclose the information. This is known as a right to "opt out" of the information sharing.

### A. *Who Must Comply?*

In contrast to the privacy notice disclosure, which must be made to customers regardless of whether information sharing takes place, the opt out notification is required only if and when an agency intends *to disclose nonpublic personal information to a non-affiliated third party* for a *non-exempted purpose.*

The opt out requirement applies only to information disclosures. If an agency does not share nonpublic personal information with other entities, or if a particular activity (such as cross-selling) does not warrant a disclosure, then the consumer is not owed an opt out notification.

Moreover, the opt out requirement applies only for disclosures to non-affiliated entities. If an agency discloses nonpublic personal information only to affiliated entities, the opt out notification requirement does not apply because information sharing with affiliates is permissible and consumers do not have a right to prevent it.

Finally, if an agency shares information with affiliates or non-affiliated entities, but it does so only for exempted purposes, the opt out notification requirement does not apply.

**B.** ***What Must Be Disclosed To Whom and When?***

Under the opt out requirement, an agency must inform its consumers that they have the right to prohibit the sharing of their nonpublic personal information with unaffiliated third parties for non-exempted purposes. This involves presenting consumers with an opt out notice and giving them a reasonable opportunity to exercise their opt out right.

There are a number of methods that can be used to offer consumers the opportunity to opt out, and an example of a satisfactory opt out notice is provided in the sample privacy form attached hereto. The methods that have been deemed reasonable under the GLBA are listed in the sample opt out clause in the attached appendices. The methods include more traditional means of corresponding with consumers (such as mailing them an opt out form on which they can check a box and sign and return the form to exercise their right to opt out) as well as electronic methods (such as providing the notification through email or a web site).

A copy of the agency's privacy policy notice must be provided to consumers along with the opt out notice.

C**.** ***What is an "Affiliate"?***

An affiliate is any entity that controls, is controlled by, or is under common ownership or control with an agency. The applicable regulations define common ownership to mean overlapping ownership of 25 percent or more. Hence, all subsidiaries of a parent company are affiliates of one another and of the parent. In addition, joint venture entities may be "affiliates" if one entity owns 25 percent or more of the joint venture or otherwise controls the affairs of the joint venture in any way. The GLBA opt out notice must be provided only if information is shared with *non*-affiliated third parties for a "non-exempted purpose."

D. ***What are the "Exempted Purposes"?***

There are several key exceptions to the opt out notification requirement. If information is disclosed to a non-affiliated third party exclusively for one or more of the exempted purposes listed below, the opt out notice is not required.

(1) <u>Exception for processing and servicing transactions</u>

A major exception to the opt out right is that it does not prohibit an agency from sharing information for the purpose of processing or completing the insurance transaction (or a related transaction) for which the information was provided. Specifically, the opt out requirements do not apply if a licensee discloses nonpublic personal financial information "necessary to effect, administer or enforce a transaction" that a consumer authorizes, or that takes place in connection with processing and servicing functions, including:

(a) Servicing or processing an insurance product or service that a consumer requests or authorizes;

(b) 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;

(c) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(d) Reinsurance or stop loss or excess loss insurance activities related to such a transaction.

"Necessary to effect, administer or enforce a transaction" includes activities: (i) necessary to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part; or (ii) necessary to underwrite insurance 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), and participating in research projects.

(2) Exception for joint agreements with service providers or for certain marketing activities

In addition to the exceptions noted above, the opt out requirement does not apply if an insurance agency provides nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the insurance agency, including marketing of the insurance agency's own products or services, or financial products or services offered pursuant to joint agreements between two or more third party financial institutions if the insurance agency fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the

confidentiality of such information. A joint agreement is a formal written contract pursuant to which two or more financial institutions jointly offer, endorse, or sponsor a financial product or service. **Independent property and casualty agents that are appointed by a number of insurance companies should enter into these joint agreements with each company for which they are appointed if the agency and the insurance company engage in joint marketing activities to offer, endorse or sponsor a financial product or service.**

(3) Other limited exceptions

There are a few other limited exceptions to the opt out requirement. Specifically, the opt out requirements do not apply when an agency discloses nonpublic personal information:

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

(b) To protect the confidentiality or security of the agency's records pertaining to the consumer, service, product or transactions, or to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;

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

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

(e) To provide information to insurance rate advisory organizations, guaranty funds, rating agencies, persons assessing an agency's compliance with industry standards, attorneys, accountants and auditors;

(f) To the extent specifically permitted or required under other provisions of law, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;

(g) To a consumer reporting agency in accordance with the FCRA;

(h) In connection with a proposed or actual sale, merger or transfer of a business or operating unit;

(i) To comply with federal, state or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by federal, state, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law; and

(j) To the extent specifically permitted or required under other provisions of law, or to comply with Federal, state or local laws, rules and other requirements.

## V. Information Reuse and Redisclosure Limitations

If an agency receives nonpublic personal information from another non-affiliated financial institution under a GLBA exception – *e.g.*, as necessary to administer or complete a transaction at a consumer's request – its redisclosure and reuse of that information for marketing purposes is prohibited. However, an agency may:

- Disclose such information to the affiliates of the non-affiliated financial institution from which it received the information.

- Disclose such information to its own affiliates, but the affiliates may use and disclose such information only to the extent that the agency would be able to do so.

- Disclose such information pursuant to an exception to carry out the activity covered by the exception under which it received the information.

For example, if an agency receives a customer list from another financial institution for claims settlement purposes or in order to provide account processing services, it may disclose such information for fraud prevention or in response to a properly authorized subpoena. **It may not disclose such information, however, to a third party for marketing purposes or use that information for its own marketing purposes.** The same rule applies, of course, to any third parties to whom the agency discloses protected information and with whom it has a joint agreement.

The limitation on the reuse/redisclosure <u>of nonpublic personal information for marketing purposes applies differently</u> to information that is received from a non-affiliated financial institution outside of an exception. For information that is received

outside of an exception, any further disclosure of such information is governed by the same rules that would govern the disclosure of that information by the financial institution from which the information received. Thus, an agency could disclose such information to affiliates (the financial institution's or its own) or to any other person if the disclosure would be lawful if made by the financial institution from which the information was received because, for example, it falls within an activity about which the consumers have been offered (and declined to exercise) their right to opt out.

## VI. Data Security and Integrity Requirement

Under the GLBA, state insurance authorities are required to establish appropriate standards for insurance agencies relating to administrative, technical, and physical safeguards to 1) insure 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. If the state insurance authority in a particular state fails to provide such standards, however, insurance agencies in that state must follow the guidelines set forth by the Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation in their joint *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule* ("Final Rule").[6]

The Final Rule provides, that insurance agencies (in the absence of state law on this subject) must do the following:

A. Information Security Program: Implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the insurance agency and the nature and scope of its activities.
B. Involve the Board of Directors/Managing Official : The Board of Directors/Managing Official must approve the insurance agency's written security program and oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.
C. Assess Risk: Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information and assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.
D. Manage and Control Risk: Design an information security program to control the identified risks commensurate with the sensitivity of the information as well

[6] 12 CFR Part 30, et al.

as the complexity and scope of the agency's activities. Each agency must consider whether the following security measures are appropriate for it and, if so, adopt those measures the agency concludes are appropriate:

1. Provide access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.
2. Provide access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
3. Develop encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
4. Develop procedures designed to ensure that customer information system modifications are consistent with the agency's information security program;
5. Develop dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
6. Monitor systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
7. Develop response programs that specify actions to be taken when the agency suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
8. Take measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.
9. Train staff to implement the agency's information security program
10. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the agency's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

E. Oversee Service Provider Agreements: Exercise appropriate due diligence in selecting the agency's service providers, require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines and where indicated by the agency's risk assessment, monitor its service providers to confirm that they have satisfied their security obligations.

F. Adjust the Program: Each agency shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the agency's own changing business arrangements, such as mergers

and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to the customer information systems.

G. Report to the Board of Directors/Managing Official: Each agency shall report to its Board of Directors/Managing Official at least annually. This report should describe the overall status of the information security program and the agency's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

## VII. Relation to State Laws

The GLBA will not supersede, alter or affect any state statute, regulation, order or interpretation except to the extent that the state statute, regulation, order or interpretation is inconsistent with any provisions of the GLBA, and then only to the extent of the inconsistency.

A state statute, regulation, order, or interpretation is not inconsistent with the provisions of the GLBA if the protection offered by the statute, regulation, order, or interpretation is greater than that offered under the GLBA.

## VIII. Enforcement

The States are required to implement and enforce the GLBA privacy requirements for insurance agents, brokers, and carriers. The federal banking and securities agencies and the Federal Trade Commission (FTC) have this same authority for the entities within their respective jurisdictions. The GLBA provides that the Attorney General of the United States may bring a civil action against any financial institution that engages in conduct constituting a violation of the Act. Financial institutions found to have violated the Act can be fined up to $100,000 for each violation and officers and directors of the financial institution may be personally liable for a civil penalty of not more than $10,000 per violation.

## Appendix I

# Sample Privacy Policy Notice

This appendix will assist in the creation of a privacy policy notice that will convey to customers your agency's practices for collecting and sharing nonpublic information. Use the sample clauses from Appendix II to develop a privacy notice that accurately reflects the type of information you collect and the type of parties that the information is disclosed.

# [*Insert name of institution*]
# Privacy Policy Notice

(as of [*insert date*])

## PURPOSE OF THIS NOTICE

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

*[If you share with third-parties for a non-exempted purpose, insert the following:]* [The GLBA further requires that we inform you that you have a right to prevent us from sharing nonpublic personal information about you with a non-affiliated third party for any purpose that is not specifically authorized by law. Your right to prevent us from sharing nonpublic personal information about you with a non-affiliated third party for a purpose that is not specifically authorized by law is called your right to "opt out" of such information sharing.]

## OUR PRIVACY POLICIES AND PRACTICES

**1. Information we collect:**

*[Insert clause 1(a) or 1(b) from the list in Appendix II labeled "Paragraph 1 Clauses," depending on which one applies to you.]*

**2. Information we may disclose to third parties:**

*[Insert clause 2(a), 2(b), 2(c), 2(d), 2(e), 2(f) or 2(g) from the list in Appendix II labeled "Paragraph 2 Clauses," depending on which best describes your disclosure practices.]*

**3. Nonaffiliated third parties to whom disclosures may be made:**

A. Nonaffiliated Third Parties To Whom Disclosures May Be Made

*[Insert clause 3A(1), 3A(2), 3A(3) or 3A(4) from the list in Appendix II labeled "Paragraph 3A Clauses," depending on which best describes your disclosure practices.]*

B. Notification of Your Right To Opt Out of Certain Disclosures

*[If you disclose information to non-affiliated third parties other than as permitted by an express GLBA exception, Insert clause 3B from the list in Appendix II labeled "Paragraph 3B Clauses." (If you do not disclose information to non-affiliated third parties other than as permitted by an express GLBA exception, then you are not required to provide this opt out notification on your privacy form.)]*

**4. Affiliates with whom we share certain information protected by the Fair Credit Reporting Act, unless you tell us not to:**

*[If you have affiliates with whom you share non-transactional, FCRA-protected information, insert the three Fair Credit Reporting Act clauses contained in "Paragraph 4 Clauses" of Appendix II. If you do not have affiliates with whom you share such information, then you can delete paragraph 4 entirely from your privacy notice and should renumber the paragraphs below.]*

**5. Our practices regarding information confidentiality and security:**

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

**6. Our policy regarding dispute resolution:**

Any controversy or claim arising out of or relating to our privacy policy, or the breach thereof, shall be settled by arbitration in accordance with the rules of the American Arbitration Association, and judgment upon the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

**7. Reservation of the right to disclose information in unforeseen circumstances:**

In connection with the potential sale or transfer of its interests, [*insert name of institution*] and its affiliates [*if any*] reserves the right to sell or transfer your information (including but not limited to your address, name, age, sex, zip code, state and country of residency and other information that you provide

through other communications) to a third party entity that (1) concentrates its business in a similar practice or service; (2) agrees to be [*name of institution*]'s successor in interest with regard to the maintenance and protection of the information collected; and (3) agrees to the obligations of this privacy statement.

**8. Customer acknowledgement and signature:**

By signing my name below, I am indicating that I have read the privacy policy of [*insert name of institution*] and that I understand its terms. No promises or representations have been made to me to induce me to sign this form.

_____

Customer Signature

Date

# Appendix II

## Privacy Policy Notice Clauses

This appendix contains sample clauses for use in satisfying your GLBA privacy notice disclosure obligations. These clauses are referred to in the sample privacy form in Appendix I. Where you have a choice of clauses that depends on the particular practices of your company, the sample form directs you to these clauses, and you should select the clause that applies to you. The numbered paragraphs of the sample form in Appendix I correspond to the sections in this appendix. Thus, where you must choose a clause on the sample form to complete Paragraph 2, you will look in this appendix for the page that lists "Paragraph 2 Clauses."

## PRIVACY POLICY NOTICE -- PARAGRAPH 1 CLAUSES

**The following clauses are used to describe the categories of information that you collect about your consumers.**

1(a) *[If you collect information about your consumers:]*

We collect nonpublic personal information about you from the following sources [*insert all that apply*]:

- Information we receive from you on applications or other forms.
- Information about your transactions with us, our affiliates or others.
- Information we receive from a consumer reporting agency.
- *[Insert any other categories of information that you collect]*

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

1(b) *[If you do not collect any information:]*

We do not collect any information about you.

## PRIVACY POLICY NOTICE -- PARAGRAPH 2 CLAUSES

**The following clauses are used to describe the categories of information that you disclose to third parties (affiliates or non-affiliates). The information in italics at the beginning of each choice tells you the circumstances in which each clause applies.**

2(a) *[If you disclose nonpublic personal information outside a stated exception, and you disclose all of the categories of information that you collect:]*

We may disclose all of the information that we collect about you, as described above.

2(b) *[If you disclose nonpublic personal information outside a stated exception, <u>but</u> you only disclose some categories but not others:]*

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

- Information we receive from you on applications or other forms, such as [*provide 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 examples, such as "your policy coverage, premiums, and payment history*"]; and
- Information we receive from a consumer reporting agency, such as [*provide examples, such as "your creditworthiness and credit history*"].

2(c) *[If you do not disclose nonpublic personal information outside of a stated exception, other than the exception for service providers and joint marketing:]*

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.[7]

2(d) *[If you disclose information under the service provider/joint marketing exception, <u>and</u> you disclose all of the categories of information that you collect:]*

We may disclose all of the information we collect, as described above, about our customers or former customers, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

---

[7] ***Note to agents:*** *This language assumes that you treat your customers and former customers the same. If you do not, you must include* ***two separate disclosure paragraphs****, one describing your practices for customers and one describing them for former customers. This is true for every paragraph in your privacy notice that describes practices that differs for customers and former customers. Thus, anytime you see a description in these clauses that groups "customers and former customers" together, you should decide whether that language is true for your company. If it is not true, then you must include separate statements.*

2(e) *[If you disclose information under the service provider/joint marketing exception, <u>but</u> you disclose only some categories of information and not others:]*

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"*].

2(f) *[If you disclose information under <u>both</u> the service provider/joint marketing exception and one or more other stated exceptions, <u>and</u> you disclose all of the categories of information that you collect:]*

We may disclose all of the information we collect, as described above, about our customers or former customers, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements. We also may disclose information about our customers or former customers as permitted by law.

2(g) *[If you disclose information under <u>both</u> the service provider/joint marketing exception and one or more other stated exceptions, <u>but</u> you disclose only some categories of information and not others:]*

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"*].

We also may disclose information about our customers or former customers as permitted by law.

## PRIVACY POLICY NOTICE --PARAGRAPH 3 CLAUSES

**The following clauses are used to describe the categories of third parties to whom you disclose nonpublic personal information. The information in italics at the beginning of each choice tells you the circumstances in which each clause applies.**

3A(1) *[If you disclose nonpublic personal information to non-affiliated entities outside of a stated exception:]*

We may disclose nonpublic personal information about you to the following types of third parties, unless you tell us not to:

- 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 non-affiliated third parties as permitted by law.

3A(2) *[If you do not disclose nonpublic personal information to non-affiliated entities outside of a stated exception, **other than** the service provider/joint marketing exception:]*

We disclose nonpublic personal information about you only to non-affiliated third parties as permitted by law.

3A(3) *[If you disclose information to non-affiliated entities under the service provider/joint marketing exception:]*

We may disclose nonpublic personal information about you, such as we have described above, to the following types of third parties that perform marketing services on our behalf or with whom we have joint marketing agreements:

- Fulfillment service providers, such as [*provide illustrative examples, such as "envelope stuffing services"*];

- Financial institutions with whom we have joint marketing agreements, such as [*provide illustrative examples, such as (include all that apply to you):*

    - *national banks and their subsidiaries;*
    - *Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities;*
    - *member banks of the Federal Reserve System;*
    - *branches and agencies of foreign banks and commercial lending companies owned by foreign banks;*
    - *organizations operating under the Federal Reserve Act;*
    - *bank holding companies and their non-bank subsidiaries;*
    - *banks insured by the FDIC;*
    - *insured state branches of foreign banks and any subsidiaries of such entities;*
    - *savings associations, the deposits of which are insured by the FDIC, and any subsidiaries of such savings associations;*
    - *federally insured credit unions and any subsidiaries thereof;*
    - *securities brokers or dealers;*
    - *investment companies; and*

- *insurance providers]*

3A(4) *[If you disclose information to non-affiliated entities under **both** the service provider/joint marketing exception and one or more other stated exceptions:]*

We may disclose nonpublic personal information about you, such as we have described above, to the following types of third parties that perform marketing services on our behalf or with whom we have joint marketing agreements:

- Fulfillment service providers, such as [*provide illustrative examples, such as "envelope stuffing services"*];
- Financial institutions with whom we have joint marketing agreements, such as [*provide illustrative examples, such as the following (include any or all that apply to you):*
  - *national banks and their subsidiaries;*
  - *Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities;*
  - *member banks of the Federal Reserve System;*
  - *branches and agencies of foreign banks and commercial lending companies owned by foreign banks;*
  - *organizations operating under the Federal Reserve Act;*
  - *bank holding companies and their non-bank subsidiaries;*
  - *banks insured by the FDIC;*
  - *insured state branches of foreign banks and any subsidiaries of such entities;*
  - *savings associations, the deposits of which are insured by the FDIC, and any subsidiaries of such savings associations;*
  - *federally insured credit unions and any subsidiaries thereof;*

- *securities brokers or dealers;*
- *investment companies; and*
- *insurance providers]*

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

**The following clause describes the right to opt out of certain information sharing with non-affiliated third parties.**

3B As we have indicated in this Privacy Policy Notice, we collect certain nonpublic personal information about you, and we may disclose that information to certain non-affiliated third parties for purposes other than those expressly permitted by the Gramm-Leach-Bliley Act and the federal and state regulations implementing that Act. If you prefer that we not disclose nonpublic personal information about you to non-affiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than those disclosures that are expressly permitted by the Gramm-Leach-Bliley Act and its implementing regulations).

If you wish to opt out of such disclosures to non-affiliated third parties, you may:

*[insert one or more of the following reasonable means of opting out:*

- *Call us toll free at (insert toll free number); or*
- *Visit our website at (insert web site address) and (provide further instructions on how to use the web site option);*[8] *or*
- *E-mail us at (insert the e-mail address); or*
- *Fill out and tear off the bottom of this sheet and mail it back to the to the address shown there; or*
- *Check the appropriate box below or on the attached form (insert a box with text next to it that says "I wish*

[8] ***Note to agents on electronic means of opting out:*** *If you use a website or an e-mail address as the only means by which a consumer may opt out, the consumer must agree to the electronic delivery of information. What this means is that, if you are currently transacting business with consumers on line, you may provide them with their opt out notifications electronically, as long as the requirements of the federal electronic signatures act are met. Appendix XI describes the requirements of the federal electronic signatures act.* ***If you are not currently transacting business with your consumers online, however,*** *it is problematic for you to offer them the opportunity to opt out only via electronic means unless you get clear permission in advance from such consumers stating that they agree to the electronic delivery of information.*

*to opt out," or refer to the **SAMPLE OPT-OUT FORM** in Appendix III)].*

## PRIVACY POLICY NOTICE -- PARAGRAPH 4 CLAUSES

**The following clauses are used to describe the required disclosures under the Fair Credit Reporting Act. If you share non-transactional information with your affiliates, you must insert the following three clauses [all three are required] into your privacy form, as directed in paragraph 4 of the sample privacy form (Appendix I).**

A. Information we can share with our affiliates, unless you tell us not to:

Unless you tell us not to, we may share with our affiliated companies information about you, including:

- Information we obtain from your insurance application, such as your income or your marital status;
- Information we obtain from a consumer report, such your credit score or credit history;
- Information we obtain to verify representations made by you, such as your open lines of credit; and
- Information we obtain from a person regarding its employment, credit, or other relationship with you, such as your employment history.

B. Our affiliated companies who may receive this information are:

- Financial service providers, such as:
  *[insert your financial service affiliates – you can describe them by name or by category, such as "mortgage lenders and brokers"]*
- Non-financial companies, such as:
  *[insert your non-financial affiliates – you can describe them by name or by category, such as retailers, direct marketers, airlines, and publishers]*
- Our other affiliates, such as:
  *[name any other affiliates or describe them by category, such as "nonprofit organizations"]*

C. How to tell us not to share this information with our affiliated companies:

If you prefer that we not share this information with our affiliated companies, you may direct us not to share this information by doing the following:

*[insert one or more of the following reasonable means of opting out:* [9]

- *Call us toll free at (insert toll free number); or*
- *Visit our website at (insert web site address) and (provide further instructions on how to use the web site option);*[10] *or*
- *E-mail us at (insert the e-mail address); or*
- *Fill out and tear off the bottom of this sheet and mail it back to the to the address shown there; or*
- *Check the appropriate box on the attached form (insert a box with text next to it that says "I wish to opt out," or refer to the* ***SAMPLE OPT-OUT FORM*** *in Appendix III)]*

[9] ***Note to agents on combining opt out forms under the FCRA and GLBA:*** *The opt out methods listed here are the same methods of opting out permitted under the GLBA. You may allow consumers to exercise both opt out rights on the same form, or you can issue two separate forms. For example, you can issue one form with two boxes – one that has text next to it saying "I want to exercise my right under the FCRA to opt out of affiliate information sharing" and one that has text saying "I want to exercise my right under the GLBA to opt out of information sharing with non-affiliated third parties."*

[10] ***Note to agents on electronic means of opting out:*** *If you use a website or an e-mail address as the only means by which a consumer may opt out, the consumer must agree to the electronic delivery of information. What this means is that, if you are currently transacting business with consumers on line, you may provide them with their opt out notifications electronically, as long as the requirements of the federal electronic signatures act are met. Appendix XI describes the requirements of the federal electronic signatures act.* ***If you are not currently transacting business with your consumers online, however,*** *it is problematic for you to offer them the opportunity to opt out only via electronic means unless you get clear permission in advance from such consumers stating that they agree to the electronic delivery of information.*

# Appendix III

## SAMPLE OPT-OUT FORM

This appendix is an example of an opt out form that you can give to customers in person to exercise their right to opt out of certain GLBA information sharing. It is an example of just one method by which you can offer the opportunity to opt out (other methods are described in the opt out notice clauses that appear in Appendix II – specifically, in clauses 3B and 4C). This particular form combines the GLBA opt out and FCRA opt out on the same form. If you are required to offer both the GLBA and the FCRA opt out notification, you can use same form, as we have done here, or you can use two different forms.

# [*Insert name of institution*]
# Opt Out Form

(as of [*insert date*])

Please read the text below and decide whether you wish to exercise your right to opt out of the information sharing described. If you choose to exercise your right to opt out, you must mail this form back to us at [*insert address*]. Your response must be postmarked no later than 30 days from the date you received this notice from us in person in order for it to be valid. If you do not mail this form back or do not mail it back within 30 days, you have not exercised your opt out right, and we can share the information described.

_____ I wish to exercise my right under the Gramm-Leach-Bliley Act to opt out of [*insert name of institution*]'s sharing nonpublic personal information about me to non-affiliated third parties for purposes other than those that are permitted by law.

_____ I wish to exercise my right under the Fair Credit Reporting Act to opt out of [*insert name of institution*]'s sharing nontransactional information about me to affiliates.

_____

___

Customer Signature Date