



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, the services of an appropriate, competent professional should be sought.

PREPARED BY THE OFFICE OF THE GENERAL COUNSEL

Memo updated as of January 2023

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 The GLBA repealed the 66-year old Glass-Seagall Act which prohibited banks, securities firms and insurance companies from being affiliated.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. It also incorporates certain minimum data security standards. Under Title V of the GLBA, the term “financial institutions” includes insurance agents and brokers. This memorandum will focus entirely on Title V of the GLBA and its impact upon insurance agents and brokers.

It is important to remember that although GLBA’s privacy and security standards 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 various model privacy and security regulations that are generally consistent with the requirements of the GLBA, but may set forth additional requirements, such as relating to breach notification requirements. Many states have promulgated individual state regulations based on the NAIC model regulations, but state laws may also change or exceed minimum requirements.

There have been a wide range of privacy and data security laws enacted in recent years in various jurisdictions. Agents should check with their state association to learn more about how your state is implementing the Gramm-Leach-Bliley Act for its insurance agents and brokers and any other state laws that may apply to your business.

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 notice that describes the manner in which their nonpublic personal information is collected, maintained, and disseminated and may need to provide subsequent notices at least annually thereafter. 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 and subsequent notice requirements. See Appendix I for a Model Privacy Form.

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 II 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.

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.

II. Information Protected by the GLBA

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, in some cases, 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. However, the FTC and several other federal agencies have created a sample privacy policy notice, which provides a safe harbor to federally-regulated financial institutions that use and abide by the terms of the sample notice. 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

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.

parties (except disclosures that fall within an exception discussed in Section IV.D.).

- (5) Any disclosures regarding affiliate information sharing that the agency is providing under the FCRA.
- (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, in some cases, 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.

D. Exception to the Annual Notice Requirement

On December 4, 2015, President Obama signed the Fixing America's Surface Transportation Act ("FAST Act" or, colloquially, the highway bill). As part of the FAST Act, Congress amended the GLBA to create an exception to the requirement that financial institutions provide customers with their privacy notice at least annually. Effective December 4, 2015, the GLBA no longer requires financial institutions to provide annual notices if they: (i) share NPI with non-affiliated third parties only pursuant to the established exemptions from which consumers cannot opt out (see Section IV.D.); and (ii) have not changed their disclosure policies and practices since their most recent consumer privacy notice. The amendments do not affect any initial notice requirements.

This exception does not, however, provide immediate relief to all insurance agencies because at least some states require that agencies provide annual privacy notices irrespective of an agency's privacy policies and practices. In the early 2000s, many states imposed privacy-related requirements to achieve compliance with the GLBA's mandates. As noted in Section VII, the GLBA does not supersede those state laws and regulations that provide greater protection to consumers. Therefore, although the GLBA's annual privacy notice requirements have changed, any state requirements remain in place until those states taken action of their own. Agencies that wish to take advantage of this exception should review their state's laws and regulations or consult with a qualified attorney.

Moreover, this exception does not apply to financial institutions that share NPI beyond the established exemptions, even if the agency has not changed its disclosure and practices. Moreover, financial institutions that use this exception still have to provide consumers with any revised privacy notices, even if the financial institution narrows the circumstances in which it discloses NPI to non-affiliated third parties.

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) Exception for processing and servicing transactions

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 Redisdisclosure 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 of nonpublic personal information for marketing purposes applies differently 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; 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 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.

⁶ 12 CFR Part 30 Appendix B et al.

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

Model Privacy Form

Below is a model privacy form developed by several federal agencies, including the Federal Trade Commission, which is a federal agency with authority over businesses such as insurance agencies and brokerages. Although use of the form is voluntary, FTC-regulated businesses will obtain a safe harbor if they use the form consistent with the FTC's instructions. It is crucial that agents and brokers ensure that their current policies and practices are consistent with their privacy policy. The requirements for relying on the safe harbor can be found [here](#). Additionally, the federal agencies have developed fillable PDFs that a business can use to create a privacy form tailored to its privacy policy. The instructions and links for the fillable PDF are available at http://www.federalreserve.gov/bankinfo/privacy_notice_instructions.pdf.

Appendix II

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