

Collier, Shannon, Rill & Scott, PLLC

Attorneys-at-Law
3050 K Street, N.W.
Suite 400
Washington, D.C. 20007



Scott A. Sinder
(202) 342-8425
Internet: ssinder@colshan.com

Tel.: (202) 342-8400
Fax: (202) 342-8451

March 31, 2000

Via Hand Delivery and Electronic Mail

Donald S. Clark
Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

**Re: Gramm-Leach-Bliley Act Privacy Rule
Proposed 16 CFR Part 313 – Comments of IIAA, NAIFA, and PIA**

Dear Secretary Clark:

On behalf of the Independent Insurance Agents of America (“IIAA”), the National Association of Insurance and Financial Advisors (“NAIFA”) (formerly NALU), and the National Association of Professional Insurance Agents, Inc. (“PIA”) (collectively “Insurance Agents”), we submit these comments to assist the Federal Trade Commission (“FTC”) in its consideration of the rules it has proposed to carry out its duty under the Gramm-Leach-Bliley Act (“GLBA” or “Act”)¹ to prescribe regulations to implement the GLBA privacy requirements included in Subtitle A of Title 5 of that Act.² The Insurance Agents are non-profit trade associations that represent almost one million insurance agents and their employees throughout the United States. Their members are independent agents who work at all levels of the insurance market and sell a full range of insurance products, including annuities.

As a general matter, the Insurance Agents believe that the FTC’s proposed rules reflect the general intent of the GLBA privacy requirements. Our comments are therefore focused most heavily on the portions of the proposed rules that raise specific questions or concerns. The comments are divided into two parts. In the first part, five overarching concerns are highlighted:

¹ See P.L. 106-102 (codified at 15 U.S.C. §§ 6801 *et seq.*).

² See 65 Fed. Reg. 11,174 (March 1, 2000).

- (1) *First*, because a consumer's ability to opt-out is the central mechanism for protecting privacy under these proposed rules, the FTC should mandate that the opt-out materials provided by financial institutions are accessible and that the right is easily and practically exercised. To facilitate this, we suggest that the examples of adequate opt-out notices provided in the rules be changed into bedrock requirements that compel financial institutions to empower their consumers to exercise their right to opt-out of information sharing practices by simply checking a box either on a paper or electronic form provided by the institution.

In this same vein, we suggest that any web site maintained by the institution include the opt-out notification and a "check-the-box" screen that can be employed by the consumer to exercise their opt-out right. We also suggest that any opt-out that is provided be effective for all accounts the consumer maintains with both the financial institution and all of its affiliates. This is especially necessary to ensure that consumer opt-outs are effective since the ability of financial institutions to share nonpublic personally identifiable information with their affiliates is not limited in any way under the GLBA.

Finally, we propose that the rules that dictate the manner in which the GLBA opt-out notification must be provided should also apply to providing the opt-out notices required under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 *et seq.*

- (2) *Second*, the FTC needs to clarify that it does not intend to regulate the conduct of insurance agents in States that do not implement or enforce their own regulations; that power is reserved exclusively to the States.
- (3) *Third*, the FTC needs to coordinate its regulatory effort with the States to ensure that the final privacy regulations of all of the pertinent regulatory bodies are uniform. Many institutions will undoubtedly find themselves subject to the GLBA privacy regulations of multiple regulators. Differences between micro-requirements could result in a compliance nightmare. We urge the FTC to ensure that this does not occur.
- (4) *Fourth*, the FTC needs to clarify the relationship between the proposed privacy rules and the pending regulations that would implement the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")(Pub. L. No. 104-191). Specifically, the FTC needs to make clear that it is not attempting to regulate the sharing

of health related information, and, moreover, that the GLBA will not modify, limit, or supersede the HIPAA regulatory regime that is being established to regulate health information.

- (5) *Fifth*, the FTC needs to clarify the responsibilities of an insurance agent and the insurance company to a particular consumer with respect to the notice and opt-out requirements.

In the second part, section-by-section comments on each of the proposed FTC rules are then provided.

Part One – Overarching Concerns

(1) *Clarify and Strengthen the Opt-Out Procedures*

Consumers' ability to opt-out of the sharing of their nonpublic personal information by their financial institution with nonaffiliated third parties is the central feature of the proposed rules. It is this ability – and this ability alone – that actually allows *consumers* to protect their privacy. Therefore, it is vitally important that the rules mandate procedures that will clearly inform financial institutions of their responsibilities under the rules, fully inform consumers of their right to “opt-out,” and make the exercise of that right as easy as possible.

To accomplish these goals requires that the FTC ensure that any opt-out notices that are provided be widely accessible and that the exercise of that right is easily achievable and practical. At a minimum, this requires the imposition of crystal clear opt-out requirements. The proposed rules contain a number of “suggestions” in the sections describing a consumer's opt-out right. Rather than offering suggestions, however, the rules should impose firm requirements that clearly delineate a financial institution's responsibilities. For example, the proposed rules provide a number of “examples” of what a “reasonable opportunity to opt-out” is.³ These examples should be firm requirements. Financial institutions should not be left to make judgment calls on what a reasonable opportunity to opt-out means; the FTC should clearly state what is required.

The rules also should make the exercise of the opt-out right as clear and simple as possible. To accomplish these two clear legislative objectives, the regulatory requirements should therefore include the following:

- (1) “Check-the-box” opt-out documents that enable the consumer to simply check a box next to a statement that they would like to exercise their right to opt-out;

³ See, e.g., 65 Fed. Reg. at 11193 (16 CFR § 313.8 (a)(2)).

- (2) Requiring that a self-addressed envelope be provided in conjunction with any written opt-out notice that is sent to the consumer by mail to facilitate consumer response; and
- (3) Requiring that the opt-out right with a “check-the-box” response be posted in an obvious and easily accessible place on any internet site maintained or operated by or on behalf of a financial institution.

Second, in addition to the requirements already imposed by the rules, all opt-out forms should plainly explain what the opt-out is and what the implications are for the consumer if he or she does not opt-out. This will ensure that the consumer has a chance to understand what opting out actually means.

Third, a consumer should only have to opt-out once to prevent all disclosures by, or among, his financial institution and all of its affiliates. In other words, even if a consumer utilizes a number of different products or services from, or establishes a number of different “customer relationships” with, a financial institution and its affiliates, the consumer should be able to fill out one opt-out form (check one box on paper, or click one box electronically) to prevent *all* disclosures related to *all* the products and services and customer relationships and *all* the affiliates. This is necessary to ensure that consumer opt-outs are effective especially because the ability of financial institutions to share nonpublic personally identifiable information with their affiliates is not limited in any way under the GLBA.

Fourth and finally, the FTC should export these opt-out requirements to the FCRA to make clear that the same requirements that apply to the provision of opt-out notices under the GLBA apply with equal force in the FCRA context for providing consumers notice of their right to opt-out of information sharing practices among affiliates. There is no policy justification for imposing different requirements on the virtually identical opt-out rights created by the two statutes.

(2) *Clarify the Applicability of the FTC Rules to Insurance Agents and Underwriters.*

The proposed rules clearly state that they do not apply to entities for which the agency does not have primary supervisory authority.⁴ Both the GLBA and the FTC’s proposed rules affirm that jurisdiction over insurance providers rests with the States.⁵ The GLBA recognizes, however, that no State is required to enforce its privacy

⁴ See 65 Fed. Reg. at 11189 (§ 313.1(b)).

⁵ See GLBA Sec. 505(a)(6); 65 Fed. Reg. at 11190 (§ 313.3(l)(8)).

requirements.⁶ It is unclear to us whether the FTC intends to attempt to enforce the GLBA requirements for insurance providers in any State in which the state authorities have failed to exercise their enforcement powers. Although the GLBA grant of enforcement authority appears to forbid any such exercise of enforcement power, the FTC has not specifically stated that its proposed rules do not apply to insurance providers. In contrast, the proposed rules of the Office of the Comptroller of the Currency – which in almost every other respect closely track the FTC’s proposed rules – contain a specific statement that they do not apply to insurance providers.⁷ We therefore request that the FTC clarify that it does not intend to attempt to enforce its rules against insurance providers to the extent that those providers are engaging in insurance activities properly regulated by the States.

(3) *Cooperate with State Insurance Authorities to Ensure Consistency in Rules*

Many life insurance agents engage in activities which cross the boundaries between regulatory authorities. For example, since many life insurance products include securities, numerous insurance agents are also registered securities brokers. Generally, the insurance activities of all insurance agents are subject to the rules promulgated by the State insurance authority in the State in which they are domiciled.⁸ Because the GLBA has imposed a new regime of functional regulation, however, many insurance agents will also be subject to the rules of other regulators when they engage in non-insurance activities. Therefore, it is critical that the FTC and other federal regulators cooperate with State insurance authorities to ensure that all privacy regulations are uniform. Otherwise, the existence of inconsistent or contradictory requirements could potentially cause a compliance nightmare for multi-function agents.

(4) *Clarify the Relationship between the GLBA and the Health Insurance Portability and Accountability Act of 1996*

The relationship between the GLBA and the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)(Pub. L. No. 104-191) needs to be clarified. The HIPAA regulations will provide detailed rules to govern the disclosure of health-related information by insurance agents and other entities. Special concerns arise in the health care context due to the unique nature of a system in which the health care needs of most workers are ensured by their employers both through state-mandated workers compensation systems and through health benefit plans. Consequently, the FTC and other agencies should make clear that the proposed rules do not apply to the sharing of

⁶ See GLBA Sec. 505(c) (denying any State that fails to enforce the privacy requirements certain benefits otherwise available under the Act).

⁷ See 65 Fed. Reg. 8770, 8789 (Feb. 22, 2000) (12 CFR § 40.1(b)).

⁸ See GLBA §505 (a)(6).

health related information. The FTC should explicitly state in a new section, similar to section 313.14 (discussing the Fair Credit Reporting Act), that the GLBA will not modify, limit, or supersede the HIPAA. Additionally, the FTC should state in the definition of “personally identifiable financial information”⁹ that it does not include health-related information, and that health related information is exclusively governed by the HIPAA. These modifications will eliminate any confusion or conflicts that could arise if insurance agents were subject to two competing sets of rules for the treatment of health-related information.

(5) *Clarify the Responsibilities of Insurance Agents and Companies in the Customer Relationship.*

The proposed rules generally contemplate that information can be freely shared for the purpose of completing transactions for which the information is provided. The rules do not exempt an institution from the privacy notification requirement if they receive information to complete a transaction and the consumer becomes their “customer” because they provide a product or service on their behalf.¹⁰ This could potentially mean that both an agent and an insurer would be required to provide separate privacy notifications even though only the agent has direct contact with the customer. The core question that this raises is whether the customer can be provided a master privacy notification that would apply to the privacy practices of all the entities that may be involved in a transaction? Clarifying that this option is available could greatly streamline the notification process in a number of contexts and thereby greatly reduce both the cost and potential consumer confusion that could be associated with providing multiple notifications.

Part Two – Section-By-Section Comments

§ 313.1 Purpose and Scope

We request that the FTC specifically state that it does not have any supervisory or enforcement authority over “any person engaged in providing insurance.”¹¹ As discussed above, this authority is vested by the GLBA in the insurance authority of the State in which the person providing the insurance entity is domiciled.

⁹ 65 Fed. Reg. at 11190, 11191 (§ 313.3(o)).

¹⁰ See 65 Fed. Reg. at 11194 (§ 313.10(a)(1)).

¹¹ See GLBA Sec. 505(a)(6) and (7).

§ 313.2 *Rules of Construction*

We believe that examples are useful in providing guidance on acceptable conduct under GLBA and the FTC's rules. As we have discussed above with regard to the explanations of rights and responsibilities under the opt-out provisions, however, we believe that these examples should be replaced with mandatory requirements. Additionally, as we note below, some of the examples provided are ambiguous and need to be clarified.

§ 313.3 *Definitions*

- (a) *Affiliate*. No comment.
- (b) *Clear and Conspicuous*. This definition is appropriate. We note, however, that the "examples" in paragraph (b)(2) are more properly captioned as "factors to be considered" in drafting a "clear and conspicuous" notice. Additionally, we recommend that the FTC provide model notice provisions to provide more specific guidance to financial institutions that fall under its enforcement authority.
- (c) *Collect*. No comment.
- (d) *Company*. The proposed rules purport to apply to any "company" subject to the FTC's jurisdiction. The definition of "company" appears to apply only to actual business entities such as corporations or partnerships.¹² The FTC should make clear, however, that a sole proprietorship is not a "company" subject to the GLBA's privacy requirements. Many small insurance agencies operate as sole proprietorships for a variety of reasons.¹³ The GLBA's requirements could pose burdens on such small agencies that they would be unable to satisfy. There is no indication, however, that Congress intended the GLBA's requirements to apply to such small businesses. For that reason, we respectfully request that the FTC clarify that it does not intend to impose these new burdens on sole proprietorships.
- (e) *Consumer*. Generally, we support the FTC's proposed definition; however, to clarify the rule's coverage, we recommend that the FTC provide an example that states that with regard to insurance, only the policyholder is to be considered as the "consumer." The policyholder typically is the person who purchases the policy and is in contractual privity with the insurer, whereas beneficiaries and insureds are not generally considered to be an insurance agent's customers.

¹² See 65 Fed. Reg. at 11189 (§ 313.3(d)).

¹³ The peculiarities of the insurance business and of the agency relationships that are prevalent are an additional reason that the FTC should make clear that it is not attempting to regulate insurance provider practices in any way. Without such guidance and without consideration of the specific issues that arise in the insurance context, insurance providers will be forced to comply with a set of regulations that do not necessarily comport with their particular industry.

- (f) *Consumer reporting agency.* No comment.
- (g) *Control.* No comment.
- (h) *Customer.* We support this definition, but, recommend that the FTC clarify that the policyholder is the “customer,” and not the beneficiary or the insured.
- (i) *Customer relationship.* This definition provides an example which states that a consumer has a continuing relationship if the consumer purchases an insurance product from the financial institution. We recommend that the example also specify that the consumer has a continuing relationship when the consumer (1) is the policyholder and (2) has received the required documentation for the insurance product. This change reflects the general insurance industry practice that a policy purchase is not effective until the insurer accepts the policy applications and issues coverage.
- (j) *Financial institution.* As discussed above, we urge that the FTC state that the term does not include a sole proprietorship.
- (k) *Financial product or service.* We object to the inclusion of the term “evaluation” in paragraph k(2) (“financial service”). The inclusion of “evaluation” broadens the scope of the term “financial services” under the GLBA. We do not believe that the FTC has the authority to expand the meaning of “financial services” in this manner. Moreover, it is not customary to treat an evaluation of an application as a service, and there is no reason why the FTC should do so. While we appreciate the concern that information contained in applications could potentially be disclosed to nonaffiliated third parties, we do not believe that either the language or intent of the GLBA reaches this information.
- (l) *Government regulator.* No comment.
- (m) *Nonaffiliated third party.* No comment.
- (n) *Nonpublic personal information.* Section 313.3 sets forth two alternative approaches to the terms “nonpublic personal information” and “public personal information.”¹⁴ Under the Alternative A approach, all personally identifiable financial information is, by definition, considered to be “non-public personal information” if it is provided to a financial institution by a consumer. The Alternative B approach to the definition of “non-public personal information,” in contrast, specifically excludes “publicly available information” that is lawfully made available to the public through the specified sources. Regardless of which definition is adopted, we believe that it is critical that the FTC take affirmative steps to ensure that whatever information is treated as public is actually public information. We also note that while several other

¹⁴

See 65 Fed. Reg. at 11190-91 (§§ 313.3(n), (o) and (p) (Alternatives A and B).

agencies also have presented these alternative definitions of nonpublic personal information, some agencies have not. We therefore specifically request that the FTC and the other agencies cooperate to ensure that a uniform standard is adopted that will adequately protect the privacy of consumers. Without a uniform standard, financial institutions will potentially face inconsistent requirements that allow them to disclose information in one regulatory context but not in another. Such a result would obviously create a compliance nightmare.

- (o) *Personally identifiable financial information.* As discussed above, we strongly urge the FTC to exempt medical information from the coverage of these rules. Therefore, the FTC should delete references to medical information in this definition. Regulations being promulgated by the Department of Health and Human Services (“HHS”) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)(Pub. L. No. 104-191) provide comprehensive standards for protecting the privacy of identifiable health information. *See 64 Fed. Reg. 59918* (November 3, 1999). Including medical information within the scope of personally identifiable financial information will only confuse financial institutions and their customers. In addition, these proposed rules may conflict with the rules being adopted by HHS under HIPAA, thereby placing financial institutions in the difficult position of having to determine which rules to comply with.
- (p) *Publicly available information.* As discussed above, it is critical that the definition chosen ensures that all publicly available information is indeed public information, and that this definition is uniform across all agency rules.
- (q) *You.* No comment.

§ 313.4 Initial Notice to Consumers

We oppose the requirement contained in paragraph (a)(1) that initial privacy notices be provided “*prior to the time*” the financial institution establishes a customer relationship. Section 503 of the GLBA provides that an initial disclosure must be made “[a]t the time of establishing” a customer relationship with a consumer. Since Congress dictated that the notice must be given at the time the customer relationship is established and not before, the FTC should clarify that the providing of the initial notice can be done at the same time that the business transaction is consummated.

Currently, paragraph (d)(2) permits financial institutions to provide notice within a reasonable time after establishing a customer relationship in connection with loan purchases, or if the consumer orally agrees to enter into the consumer relationship and the consumer agrees to receive the notice thereafter. Paragraph (d)(2) should be modified to allow insurance providers to provide notice at the same time as the insurance policy is delivered to the policyholder. This change would better coincide with industry practice because in the insurance industry, the issuance of the insurance policy denotes the time

when the company is obligated to provide insurance as well as when the customer relationship is formally established.

Finally, we believe that it is better to mandate specific procedures for the delivery of the required notice and opt-out form. Accordingly, paragraph (d) should be redrafted as an affirmative requirement to deliver the notice required by paragraph (a):

- (1) in person, or
- (2) by regular letter mail, or
- (3) by electronic mail if agreed to by the consumer.

§ 313.5 Annual Notice to Customers

We agree with the paragraph (c) directive that a consumer may be deemed to no longer be a customer if the financial institution has not communicated with a customer for 12 consecutive months, and that financial institutions should have the discretion to make this determination.

§ 313.6 Information to be Included in Initial and Annual Notices

We are generally supportive of this provision and believe that it tracks the GLBA requirements.

§ 313.7 Limitation of Disclosure to Nonaffiliated Third Parties

As discussed above, the examples in paragraph (a)(3) should be changed into mandates. This can be accomplished by rewriting paragraph (a)(3)(i) to read:

“You must provide a consumer the reasonable opportunity to opt-out by mailing, either by traditional letter mail, or by electronic mail if agreed to by the consumer, the notices required in paragraph (a)(1) of this section to the consumer, and allowing the consumer 30 days to opt-out.”

§ 313.8 Form and Method of Providing Opt-Out Notice

As discussed at the outset, we recommend that the FTC make the illustrative examples of an adequate opt-out notice in (a)(2) affirmative mandates. Paragraph (a)(2)(ii) would thus read:

“To provide a reasonable opportunity to opt-out you must do one of the following: . . .”

The examples would then be the required choices for complying with the opt-out notice requirement. In this regard, we also believe that providing a self-addressed envelope should be required under both (a)(2)(A) and (B).

As with section 313.4(d) above, paragraph (b)(1) should be redrafted as an affirmative requirement to deliver the notice required by paragraph (a):

- (1) in person, or
- (2) by regular letter mail, or
- (3) by electronic mail if agreed to by the consumer.

The word “examples” in paragraph (c)(3)(i) should be deleted to make a change-in-terms notice required in the two circumstances listed.

Paragraph (e) should be amended to clarify that once a consumer opts-out, that opt-out applies to each service product, service, or customer relationship he or she has, or subsequently has, with the financial institution and/or any of its affiliates.

Finally, we are fully supportive of the requirement that a consumer’s revocation of his or her decision to opt-out must be in writing or in electronic form. We believe that this is necessary to insure that any revocation of a previously exercised right is not based on a misunderstanding. Because financial institutions are permitted to require the opt-out to be exercised in writing, they should be required to receive the revocation in some written form.

§ 313.9 Service Provider and Joint Marketing Exceptions

No comment.

§ 313.10 Exceptions for Processing and Servicing.

We believe that the exceptions provided generally conform to section 502(e) of the GLBA. We urge, however, that some of the specific language of the GLBA that has been omitted be preserved. The words “in connection with” which appear in section 502(e)(1) should be inserted to modify paragraphs (a)(2), (3) and (4), as they do in the GLBA. We believe that this is an important addition because Congress intended the processing exception to apply both “as necessary to effect, administer or enforce a transaction requested or authorized by the consumer” and “in connection with servicing or processing a financial product or service requested or authorized by the consumer.” This latter statutory clause is essential because it broadens the scope of the initial authorization to ensure that sharing that is done “in connection with” the requested service or product also is fully permissible. If this clause is excluded in the rules, we are concerned that it may create a gap which could interfere with the efficient delivery of products and services to consumers.

It also is important to note that we believe that the special insurance provision set forth in (b)(2)(v) that has been included is sufficient to enable agents and brokers to process insurance applications and service their clients under those contracts.

§ 313.11 Other exceptions

With regard to paragraph (a)(1), the FTC has asked whether a financial institution should require a consumer to provide such consent in writing. For the reasons presented above with regard to a consumer's revocation of his or her opt-out, we believe that a consumer's consent should be in writing to ensure that there is no misunderstanding regarding the consumer's revocation of his or her rights.

§ 313.12 Limits on Rediscovery

No comment.

§ 313.13 Limits on sharing account number information

The FTC should clarify that the term "transaction account" does not include an insurance policy. There does not appear to be any basis for treating an insurance policy as a transaction account. We also recommend that the FTC permit financial institutions disclose consumer account numbers or similar forms of access numbers or access codes in an encrypted, scrambled or similarly coded form if (1) the consumer consents and (2) the disclosure is necessary to process or service the transaction requested or authorized by the consumer. This exception would be consistent with the legislative history of the GLBA.

§ 313.14 Protection of the Fair Credit Reporting Act

We recommend that the FTC clarify that the FCRA provides overlapping requirements that are unaffected by these proposed rules.

§ 313.15 Relation to State laws

Paragraph (b) of this proposed rule purports to extend the GLBA statutory preemption to the FTC's proposed rules. We do not believe that any such extension is warranted, especially in light of the several departures from the statutory framework that are noted above.

§ 313.16 Effective date

The FTC has proposed an effective date of November 13, 2000. It is our understanding that many other commentators will request that this date be extended to provide them with the opportunity to make the operational changes necessary to implement the rules. We join in this request in part because a short extension also would

better enable the states to make the necessary statutory and regulatory amendments that are necessary to empower their insurance regulators to enforce the GLBA privacy requirements.

We would be happy to provide any additional comments or materials that would assist the Commission with its deliberations.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott A. Sinder", is written over a horizontal line.

Scott A. Sinder

John J. Manning

Counsel to IIAA, NAIFA, and PIA