American Insurance Association

1130 Connecticut Ave. NW
Suite 1000
Washington, DC 20036
202-828-7100
Fax 202-293-1219
www.aiadc.org

May 29, 2007

Office of the Comptroller of the Currency
250 E Street, S.W.; Mail Stop 1-5
Washington, DC 20219
Docket Number OCC-2007-0003

Federal Trade Commission/Office of Secretary
Room 135 (Annex C); 600 Pennsylvania Avenue
Washington, DC 20580
FTC File No. P034815

Jennifer J. Johnson
Secretary, Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551
Docket No. R-1280

Robert E. Feldman
Executive Secretary,
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429
Attention: Comments

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
Attention: OTS-2007-0005

Nancy M. Morris
Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549
File Number: S7-09-07

Mary Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Eileen Donovan
Acting Secretary of the Commission
Commodity Futures Trading Commission
1155 21st Street
Washington, DC 20581

Re: Model Privacy Form – Interagency Proposal for Notice under the Gramm-Leach-Bliley Act

Dear Ladies and Gentlemen:

The American Insurance Association (AIA) is a trade association which represents property and casualty insurers doing business across the country and around the world. Although the proposing agencies are not the functional regulators of insurers, insurers are "financial institutions" under the Gramm-Leach Bliley Act (GLBA). Some integrated financial institutions do business across multiple sectors of the industry – banking, securities and/or insurance. As such, the Interagency Proposal for a Model Privacy Form (Proposed Model or Proposed Form) interests AIA members.

It would be a disappointing irony for the same legislation that enabled the existence of truly integrated financial institutions not to provide safe harbor status to one single integrated privacy notice for such institutions. As drafted, the Proposed Model appears to be aimed mostly at depository institutions. For other sectors of the financial services industry to consider using the Proposed Form it must be modified to be meaningful for their business. While the insurance industry presents unique concerns given the manner in which it is regulated, there may be ways to take some of these concerns into account when drafting the text and when outlining the rules to govern the Proposed Model. These comments are organized in three sections: content concerns, formatting concerns and safe harbor status. They are followed by an Appendix showing suggested alternative language for your consideration.

A. Content of Proposed Model Form

1. Overview – Content of Model Form

In order for various types of financial institutions to be able to take advantage of the safe harbor notice and for that notice to provide meaningful and accurate information to customers, the model notice should:

- contain terms that are generic with applicability across sectors;
- provide a limited menu of alternatives, from which the institution may select those that make sense for their business;
- allow an institution to omit words or phrases that are inapplicable to its business or practices; and/or
- allow the institution the freedom to tailor its notice as necessary, within the structure of the model notice form.

For example, activities like "deposit[ing] money" or "apply[ing] for a loan" do not make sense in an insurance context. However, "applying for services" or "initiating transactions" are general descriptions that make sense for our industry as well as others.

A more standardized format may aid the reader. However, to really meet the intent of GLB privacy provisions, the notice should allow financial institutions to convey information in a way that provides meaningful choice. Indeed, according to the House Committee Report from June 15, 1999, disclosure rules are to be aimed at permitting "customers to readily compare differences in the privacy practices and policies among financial institutions."[1] Too much boilerplate language takes away some of the basis for customers to compare privacy practices.

Of course, this approach cannot be effectively implemented under a take-it-or-leave-it safe harbor. A mandate that the entirety of the notice be taken verbatim from the Proposed Form disregards differences in sectors of the industry, in privacy and business practices and in ways of communicating with customers. Modifying the proposed safe harbor form to allow for greater flexibility is in everyone's best interest – customers get a better idea of the kind of sharing they are to expect and financial institutions can feel more secure that the notices they are sending more accurately reflect their business practices.

2. Essential Suggested Revisions – Content of Proposed Model

Below AIA discusses the most crucial concerns with the Proposed Model.

[1] See, H.R. Report No. 106-74, at 107 (1999).

WHAT? Not all financial institutions collect customers' Social Security numbers or income information. To include them where they are not collected or shared would not only be inaccurate, but may cause customers undue concern.

Not all financial institutions call their products "accounts." The term "transaction history" may be suitable to several sectors and cover the applicable activities. Similarly, reference to closing an account could be better phrased other ways like "when you are no longer a customer." The final sentence in this area could be simply put: "We apply the same practices to current and former customers."

Financial institutions are not required to give former customers annual notices. However, their privacy notice must indicate how they treat former customers - there is no requirement that they be treated identical to existing customers.[2]

"Information from consumer reports" could replace "credit history and credit scores." Many financial institutions gather information from consumer reporting agencies. Such collected information may be broader than credit information. For example, in the property and casualty insurer context it may also include loss history reports and motor vehicle reports.

As drafted, the Proposed Model contains no definition of "personal information." That term does not include data that is publicly available; the notice could indicate that the information at issue is nonpublic. Additionally, a financial institution should have the ability to specify that it is addressing only "financial" information in this notice. Or, it should have the ability to tailor this notice to address all its privacy notice requirements under state and federal law. Please see the safe harbor remarks below.

HOW? The Proposed Model should not only address whether a customer may limit sharing, but also its use. An institution may want to go beyond addressing sharing to include collection and use in order to provide a complete description of its organization's practices regarding personal information.

REASONS With respect to "For our affiliates to market to you," a complete response also needs to take "use" into account.

The term "creditworthiness" does not apply across financial services sectors. Perhaps a number of alternatives could be available to institutions, including "insurability." Or, if a more generic term is preferred, maybe "transactional experience" is useful. Or, perhaps consider "information other than information about your transactions with us." Further, since "everyday business purpose" is defined, this may not be necessary. See below.

With respect to the reference to nonaffiliates, the ability to limit does not extend to activities such entity engages in on behalf of the financial institution.[3] The Proposed Form should be modified to make this clear.

---

[2] See NAIC Model Privacy Regulation Sections 6(B)(1) and 7(A)(4).

[3] See Section 13(b) of the Federal GLB Regulations and Section 14(B) of the NAIC Model Privacy of Consumer Financial and Health Information Regulation.

CONTACT Not every financial institution grants its customers the opportunity to opt out via phone number. Federal law does not require financial institutions to accept requests to opt out in any particular medium. Also, some financial institutions may prefer to have customer information sharing decisions in writing. Therefore, the proposed notice form should not mandate the inclusion of telephone numbers, web addresses or any other particular mode of contact.

The 30 day language assumes that is the "reasonable" amount of time under the law. The law does not require financial institutions to grant their customers any particular amount of time to exercise that opportunity.

More importantly, the 30 day language could be read to apply to both the annual notice and the initial notice. However, it should apply only to initial notice because the law does not require a yearly moratorium. Therefore, it is neither appropriate that a model form mandate a moratorium against sharing information for any particular amount of time nor that it force financial institutions to cease sharing information when providing their annual notices if their customers did not previously opt out of the sharing.

SHARING The term "account" will not be applicable for all financial products and services. With this in mind, the question of how often the notice is required should be rephrased, perhaps in terms of "when you first become a customer."

The legal data security requirements are framed in terms of "administrative, procedural and physical safeguards." Therefore, rather than mention "secured files and buildings" it is more accurate to reference "physical safeguards."

The information supplied relating to the timing for collecting personal information should allow for using the terms applicable across the financial services industry. For example, terms like "initiate transactions with us" or "apply for services with us" are more generic than "open an account or deposit money" which seem bank-oriented. Similarly, "applying for a loan" would not apply in the insurance context.

If the field dealing with reasons all sharing cannot be limited is retained, despite concerns mentioned below, please consider the difference between sharing and use discussed in HOW above.

DEFINITION On the one hand it looks like a financial institution may indicate the "categories of its affiliates," but on the other it seems that a specific format must be used. Flexibility is very important here. Consider, for example, an integrated financial services company which may want to describe the business of the kinds of affiliates with whom it may decide to share – securities, lending, life insurance, and/or property and casualty insurance. The currently proposed limited format for listing affiliates is too restrictive. In this way, the Proposed Model may disallow an approach that comes closer to fulfilling the intent of the GLB notice obligations. Through a description of the kind of internal sharing, the customer will get a better sense of the kinds of entities with whom its company is sharing (as compared to sample list of affiliate names).

CHOICES The opt-out portion of the notice is over simplified.

The proposed model does not contemplate a partial opt out, where a financial institution may allow the customer to select a choice to limit some but not all kinds of sharing and some but not all kinds of nonpublic personal information.

With respect to the first check box, "creditworthiness" alone does not take into account the non-lending activity of financial institutions. This entry also does not make it clear that transaction experience may be shared regardless.

With respect to the second check box, consider that a customer may have relationships with multiple affiliates within a family of companies. The notice should not lead the customer to believe that it may choose to restrict in those instances, but rather only with those affiliates with whom it does not have a relationship.

Also, current law does not require a "renewal notice" after 5 years. Rather, it indicates that the financial institution has the option to approach the customer with another privacy notice in 5 years. From an operational perspective, a financial institution may find it easier to treat a customer's opt out as a permanent election rather than to treat it as expiring in 5 years. The financial institution should not be forced to ask the customer her opt out decision again.

With respect to the third check box, the nonaffiliated opt out should be limited to non-financial activity, since financial activity would fall within the joint marketing exception.[4]

3. Other Important Suggested Revisions – Content of Proposed Model

(a) Flexibility

There are numerous instances throughout the form where it would be helpful for financial institutions to tailor their notices to emphasize features of their privacy practices. The form will allow customers to compare privacy policies while still giving them choice in the marketplace. Identical wording for notices provided by every financial institution is not required – or even necessarily contemplated – by the federal law. Nor does identical wording provide customers any meaningful basis for comparing the privacy policies of the financial institutions. Some flexibility within the context of the safe harbor format would allow for the institution to convey non-prescribed information. This kind of adaptable template is not only less rigid, but it benefits everyone involved.

Flexibility is not just a matter of preference; it may be needed for financial institutions to comply with state laws. For instance, approximately 16 states have privacy laws which mandate insurers to provide customers with notice of their "access and correction" rights.[5] Other states require disclosures about practices relating to medical information. Additionally, there are small, but necessary, deviations in state-required language, as is the case in Montana.[6]

The need for adaptability does not all arise from substantive legal requirements addressing notice content. Also consider format requirements. For example, the California specific opt-in/out form

[4] See 15 U.S.C. Sec. 1681s-3.
[5] See the NAIC Insurance Information and Privacy Protection Model Act (1982).
[6] See MCA 33-19-307.

wording and envelope requirements do not match those contained in the Proposed Model.[7] Further, the California form must have a readability score of 50.[8] Other states have font requirements.

Variable text, allowing for flexibility, is shown in the attached Appendix by brackets [ ]. Also, please see discussion below about all-or-nothing safe harbor approach.

WHY? This field is not mandated by GLBA, but it may provide a useful context about the reason for the notice. Some financial institutions may want to describe their relationship, the applicable law (perhaps including state law), their practices and the notice obligations to their customers in their own words.

Notice should only be required to be provided to someone with whom an institution has a business relationship. For insurers, such people are "customers" as distinguished from "consumers."

WHAT? Allowing financial institutions the ability to tailor the bullet points to reflect their actual practices will make for more accurate notice and for more meaningful customer choice. For example, insurers may also want to refer to things like past insurance claims or reports of accidents as well as home inspections. By tailoring the information to better match the kind of sharing, the customer will have a fuller understanding of the information collected and shared. Within the structure of a common template, the financial institution should have the flexibility to describe its practices to those with whom it has a business relationship.

Historically, a financial institution may have carefully crafted its notices to reflect the information gathering process to provide the customer with a context for the collection and use of nonpublic personal information. It should continue to be able to convey this kind of information – and with the peace of mind of being within a safe harbor.

To the extent the Agencies are willing to allow for a menu approach for integrated financial services companies, the securities-related "assets and investment experience" should also appear on this list.

WHAT/HOW Consider whether the statement about former customers more closely fits with the information conveyed in the HOW section of the Proposed Form.

WITH WHOM A financial institution may decide it will be easier for the customer to understand why sharing would occur with any of the listed parties if there is further explanation. Since this may aid in their understanding, this option should be allowed. To illustrate, under the affiliate heading, a company might provide examples like "sharing with affiliates in order to provide the product or service best suited to your needs." Also, under the nonaffiliated heading, a company might include "sharing with other companies in order to process your payments, respond to government or other legal requests or provide other services you request." Finally, under joint marketing, examples may include "providing you the opportunity to investigate other products or services you may find of interest." (See DEFINITIONS comment below for more discussion of WITH WHOM.)

[7] See Cal. Code Regs. tit. 10, Sec. 2689.8.
[8] See Cal. Code Regs. tit. 10, Sec. 2689.4(6).

Personal lines property and casualty coverages are often written under separate policies through separate companies – customers may not just be placed into a particular tier within one company, but into one company within a group. An underwriter generally is not an employee of only one insurance affiliate. He typically looks at a whole package or range of options across the family of companies and not just at a particular writing company – the writing company is more of a technicality. This occurs for several reasons, but is in large part due to the nature of state regulation. Even very restrictive legislation such as California Senate Bill 1 recognized sharing within the context of companies under common management (or companies sharing one managing group, with only one company having employees). To the extent there are not separate employees among affiliated insurance companies, there is no transfer of knowledge. A financial institution may want to explain the nuances of the issuing/managing company environment. For example, it may want to express that within the family of companies the same processing systems and employees are used to maintain coverage.

REASONS Financial institutions should have the flexibility to provide more detail than a "yes" or "no" answer in order to provide customers with more accurate responses. Customers are more likely to get a better understanding of a financial institution's privacy practices if the institution is given the opportunity to provide more detail, making the notices more meaningful and understandable.

SHARING The information relating to how information is collected is another area where it would be helpful for institutions to be able to provide the information that makes the most sense in the context of their business. Furthermore, it may be useful to insert a placeholder for optional additional questions and answers, which a financial institution feels aids it in describing its practices to its customers.

DEFINITION To the extent the "everyday business purposes" definition is maintained, consider expanding the options to allow for "contract administration" as well as for a variable field. At present, the list does not necessarily include a broad sample of insurer uses.

In terms of improving readability, consider adding a WITH WHOM area to the form and removing the DEFINITIONS all together. Customers may not pay as much attention to a seemingly technical "Definitions" section as they would a section that gets at where their information is going. The everyday business purpose is already addressed under HOW and REASONS and could be modified slightly in those areas.

MULTIPLE References to affiliates and nonaffiliates appear in a number of places in the Proposed Model. See REASONS, DEFINITIONS and CHOICES. A financial institution may want to use words to describe the corporate ownership relationship that it may believe will be less technical for the customer. For example, it should have the flexibility to refer to sharing "with affiliates" as "among XYZ companies" and "with nonaffiliates" as "outside of the XYZ family of companies."

CHOICES Under the Proposed Form, a financial institution may not offer its customers the ability to partially opt-out of sharing certain types of nonpublic personal information or certain nonaffiliated third parties. To the extent there is no place to accommodate a partial opt-out, the form lacks adequate flexibility.

(b) Streamlining