March 31, 2000

Mr. Jonathan G. Katz, Secretary
U.S. Securities and Exchange Commission
450 5th Street, NW
Washington, DC 20549

Re: Regulation S-P: Privacy of Consumer Financial Information, Release Nos. 34-42484,IC-24326, IA-1856; File No. S7-6-00

Dear Mr. Katz:

Please accept this comment letter on behalf of the North American Securities Administrators Association, Inc. ("NASAA")[1]. NASAA appreciates the opportunity to comment on this very important issue of privacy of consumer financial information. In light of the growing consolidation and affiliation among the various industries and entities that offer financial services to consumers, the sharing of consumer financial information among such entities is going to increase and can be lucrative when sold to nonaffiliated entities. In many respects, a conflict can develop. The sharing of such information may be helpful and efficient for consumers, but such sharing could also result in unwanted access to personal information.

STATES' RIGHT TO ADOPT MORE STRINGENT PRIVACY REQUIREMENTS

Today we comment on the rules proposed by the Commission to implement the privacy provisions under the Gramm-Leach-Bliley Act ("GLBA"). We also acknowledge, however, that GLBA permits the states to adopt their own more stringent privacy requirements. While we defer to state legislatures to determine whether additional protections are necessary for their citizenry, we applaud and support the efforts put forth by the Commission as well as the other federal agencies charged with implementing the privacy provisions under GLBA within the very brief timeframe. NASAA offers the following comments in response to the Commission's solicitation for input on the proposed rules.

---

[1] NASAA, the oldest international organization devoted to investor protection, was organized in 1919. It is a voluntary association with a membership consisting of the 66 state, provincial and territorial securities administrators in the 50 states, the District of Columbia, Canada, Mexico and Puerto Rico. In the U.S., NASAA is the national voice of the 50 state securities agencies responsible for investor protection and the efficient functioning of the capital markets at the grassroots level.

EXAMPLES AS GUIDANCE; NOT SAFE HARBORS

The Commission invites comment on whether including examples within the rules is useful. We support the Commission's use of examples in the rules to provide practical guidance to financial institutions. While providing guidance, the examples also permit financial institutions flexibility in their compliance approaches. The Commission also chose not to propose that compliance with the examples would provide a safe harbor for financial institutions. We strongly support the Commission in this decision.

After more than 40 years, GLBA has removed restrictions on financial institutions from selling certain products and merging or affiliating with certain companies. It is very difficult, therefore, to predict the way these companies will evolve and share information in the future. In light of this uncertainty and the practices that will develop among financial institutions, individual institutions should be regulated by their specific actions and specific privacy-sharing plans rather than on general safe harbors based on an unknown landscape.

Notwithstanding the desire to avoid establishing safe harbors at this preliminary stage and although the examples are helpful, we suggest that for some provisions of the final rule, minimum thresholds of required conduct would be appropriate. Otherwise, a financial institution may choose to ignore the example or examples provided in instances where the examples should indicate minimum standards. NASAA respectfully suggests that under certain provisions of the proposed rules the Commission consider including the criteria set out in the examples as required conduct. In addition, the facts and circumstances of each individual situation shall determine whether there is compliance with any particular provision.

DEFINTIONS (Section 248.3)

(b) Broker and (l) Dealer :

The definitions of broker and dealer as included in the proposed rules are important for two reasons. First, these definitions provide consistency and clarity under the securities laws because they are the same definition as presently included under the Securities Exchange Act of 1934. Secondly, as the text of the release makes clear, the definitions apply to all persons within the meaning of those terms whether or not the broker or dealer is registered under the Exchange Act.

Registration requirements under the Exchange Act serve a different purpose than the privacy requirements created under GLBA. For example, an entity, although meeting the definition of broker under the Exchange Act, may be exempt or excepted from the requirement to register under the Act. Despite this exempt or excepted status, the entity still generally performs the services of a broker, including having access to investors' personal financial information. In addition, an entity that should be registered but otherwise is not registered as a broker is nevertheless still a broker and has access to

personal financial information. For purposes of protecting investors' privacy rights, all brokers and dealers whether or not registered should meet the GLBA privacy requirements.

(c) Clear and conspicuous:

We are concerned about the proposed definition of **"clear and conspicuous"**. The notice requirements are some of the most important parts of the rules with respect to consumer privacy protection. If a consumer is not given effective notice that he or she is entering into a relationship where his or her private financial information might be shared with others, the consumer may also not know of his or her opt out rights. For that reason, we believe that the language of the rule specifying that the notice "be **reasonably** understandable and designed to call attention to the nature and significance of the information contained in the notice" is vague and creates an uncertain standard. On the other hand, we think that the examples provided in the rule are very helpful. Unfortunately, as previously mentioned, examples do not have to be followed. Given the importance of this provision we suggest that the Commission consider providing affirmative guidance to financial institutions to provide notice as specified in the examples, rather than leaving it up to the financial institutions to decide whether or not to follow these examples. Therefore, we would respectfully suggest including most, if not all, the criteria set forth in the examples as necessary conduct under the definition.

(g) Consumer:

The Commission incorporates in the proposed rules the definition of consumer as set forth in GLBA. In addition, the Commission, in the release, states "an individual will be deemed to be a consumer for purposes of a financial institution if that institution *purchases* the individual's account from some other institution." This statement in the release clarifies that even if an individual does not *obtain* (the wording from GLBA) a financial product or service from the financial institution directly, the individual may still be a consumer of the financial institution. However, we would respectfully suggest that the clarification falls short because it uses the term "purchases", which suggests only a single type of scenario and thus, is far too narrow. For example, if a financial institution merges with another financial institution, agrees to swap information with another financial institution or otherwise obtains the individual's account from another institution, the individual should be deemed to be a consumer of that second financial institution. We encourage the Commission to expand the explanation in the release to address these other scenarios.

(j) Customer:

It appears under the rules an individual could be classified as a consumer for certain products and a customer for other products. Once a consumer also becomes a customer of a financial institution the individual will receive an initial and annual notice of the institution's privacy policies and practices and additional protections. We believe that the rule should state that once an individual becomes a customer of a financial

institution that financial institution must treat that individual as a customer for *all* purposes under the privacy rules. If not, the individual's personal information could possibly be shared under broader circumstances as a consumer rather than a customer.

(k) Customer relationship:

This definition is dependent upon the interpretation of a "continuing relationship". We do not believe it will always be obvious at the beginning of a relationship between a consumer and a financial institution that the relationship will be "continuing". For example, a fee-only financial planner charges a one-time fee for services to a client. The fee is paid and the services rendered with or without signing an advisory contract but, regardless, the contract is complete when the services are rendered. The client may return each year or several times a year and yet, under the definition, the client may not be considered a customer. Example (2)(iv) provides a similar type arrangement but it relates to effecting a securities "transaction" not advisory services or financial planning.

Similar to the definition of clear and conspicuous, we recommend the Commission include the examples in this definition to set forth minimum circumstances when a "continuing relationship" would be established. Additionally, we would suggest including an example similar to the fee-only scenario mentioned above.

(t) Nonpublic Personal Information; Personally Identifiable Financial Information; Publicly Available Information:

We note that the Commission's definitions of "nonpublic personal information", "personally identifiable financial information" and "publicly available information" are mutually dependent. One way we read the above-referenced definitions to interact is as follows. Personally identifiable financial information is by definition nonpublic personal information if it includes any or all of the information an individual consumer provides to a financial institution or if it is a list of consumers derived using any personally identifiable information. However, nonpublic personal information does not include publicly available information except if provided in a certain manner.

We would like to highlight three specific issues that are raised because these definitions are interdependent.

Issue One: It is unclear whether a consumer's or a customer's name is itself personally identifiable financial information. We note that there is an exception from the definition of personally identifiable financial information if the information is *derived* using only publicly available information. However, we also acknowledge footnote 31 in the release, which states:

> Nonpublic personal information does include publicly available information that is disclosed in a manner that otherwise indicates the individual is a financial institution's consumer. See proposed § 248.3(t)(2)(i). We believe that, in most cases, sharing information (including publicly available information) about a consumer with a third party identifies the individual as the institution's consumer.

The second sentence of the footnote appears to imply that by giving out merely the name, address and public phone number of a **single** consumer such action itself "identifies" the individual as the financial institution's customer. But, the first sentence of this footnote cites to section 248.3(t)(2)(i), which states that nonpublic information does **not** include publicly available information **unless** the information "(a) when disclosed relating to consumers is a list or grouping of consumers, which list is *derived* using *personally identifiable information* or (b) when disclosed relating to customers is disclosed in a manner that *indicates* the individual is or has been a customer." Without affirmatively stating that a consumer name (which, by definition, is obtained by a financial institution from an initial action taken by the individual and not the financial institution) or a customer name is itself personally identifiable financial information it appears either a consumer or a customer name could be embodied within a list and be considered publicly available information as long as the customers were not "identified" as customers and the consumers were not contained in a list with using *personally identifiable information*. This is very confusing and permits financial institutions to avoid compliance with the requirements for notice and an opportunity to opt out.

We provide the following example to illustrate that this rule needs to be modified:

Bank Alpha Report	**Bank Beta Report**
Individual: Bob Jones	Customer: Bob Jones
Address: 10 Main Street	Address: 10 Main Street
Washington, DC 20002	Washington, DC 20002
Phone: 202-555-1212	Phone: 202-555-1212
House Valued At: $500,000	House Valued At: $500,000
Report generated by Bank Alpha	*Report generated by Bank Beta*
April 20, 2001	*April 20, 2001*

In this example, Bank Alpha need not comply with GLBA provisions but Bank Beta must. "Information disclosed in a manner that indicates the individual is or has not been your customer" would not necessarily protect a customer's anonymity if the only thing a financial institution would need to do is not label the list as a customer list or not "identify" the individual as a customer. In addition, what if a financial institution intermingles names from a phone book search with consumers and customers?

Can an inference be drawn from the fact that the financial institution has such a list and is willing to provide it to others that it must contain consumer or customer names and thus is nonpublic personal information. Does a single name have more or less protection than the same name when included in a list? Is it different for consumers vs. customers?

We believe it is the rule's intent, but encourage the Commission to make Regulation S-P clearer, so that, at a minimum, a list of *customer*s, regardless of the information contained on that list, is always personally identifiable financial information.

Issue Two: The current proposal would allow an institution to freely disseminate information it gathered from an application or other data it collected from a consumer's or customer's account so long as that data is publicly available. The Commission, however, seeks comment on whether the proposed definition of *publicly available information* should treat information that is available to the public form other sources as *nonpublic information* unless the institution itself obtains the information from the public source. The FTC proposed two alternative definitions for *nonpublic information:* Alternative A and Alternative B. In a letter to the FTC, we supported Alternative A which would require the institution to actually obtain the data from a public source to allow it to disseminate it outside GLBA regulations. We respectfully recommend the Commission use this approach.

An institution should be allowed to share information without complying with these privacy rules simply because the information exists publicly somewhere else, no matter how esoteric the source or sources. Various types of information are contained within public documents, however, the information may not be readily available, nor categorized or sorted in such a manner to make it truly accessible. We recommend that the Commission require the information to be collected by a financial institution itself from a public source to classify the information as *publicly available information*. If the "alternative approach or rule" were adopted, a bright-line test would be created for financial institutions. A financial institution would know if it collected the information from public sources, the information can be distributed without having to comply with GLBA rules. If the institution collected the information as part of an application or other methods defined in the personally identifiable information, the institution must comply with the rules.

Issue Three: As previously noted, the rules seem to establish or provide for an interpretation that information on a particular consumer or customer may be treated differently than a consumer or customer "list". Although what is meant by a "list" may be obvious in a paper world, it may not be so obvious in an electronic one. How would a steady "feed" of names between two computers be treated if the names were sent one at a time but one after another? We recommend the Commission consider defining *list* or develop other rules to prohibit institutions from using technology to send one name in separate e-mails in milli-second bursts or other such means of delivery of information that would evade the rule's purpose.

INITIAL NOTICE TO CONSUMERS OF PRIVACY POLICIES AND PRACTICES REQUIRED (Section 248.4)

(a): When initial notice is required.

It appears section 248.4(a)(1) mistakenly references 248.4(d)(1) instead of 248.4(d)(2).

(c): When you establish a customer relationship.

We note that one of the examples the Commission provides in this section indicates that a customer relationship is established when a consumer "opens a brokerage account with [a financial institution] under [a financial institution's] procedures". We recommend that the Commission require a financial institution to make clear to the consumer at what point in time a person is to be considered as having "open[ed] a brokerage account with [it] under [its] procedures."

(d): How to provide notice.

(2) Exceptions to allow subsequent delivery of notice. We question allowing a consumer to enter into a customer relationship orally and permitting the financial institution to provide for delivery of the notice of the institution's privacy policies and practices at a subsequent time. As previously mentioned, we believe that from the view of a consumer, one of the most important parts of these rules is the ability to get notice of how a financial institution intends to share a consumer's nonpublic information and either (a) decide not to do business with the financial institution or (b) decide to enter into an agreement but not allow the financial institution share financial information with nonaffiliated third parties.

Congress emphasized the importance of the notice by mandating that the privacy notice and the opt out opportunity be provided in writing to the consumer and that the notice be given to a consumer before he or she makes a decision to buy a financial institution's service or product. To allow a financial institution to delay providing this important information to a consumer by simply obtaining an oral agreement from the consumer eviscerates the impact of GLBA and opens the opportunity for less scrupulous companies to "fast talk" a consumer into deferring receipt of the notice until after the customer relationship has been established. As drafted, this rule will be providing opportunity to a small portion of the industry that is well known for cold calling and high-pressure sales tactics to avoid timely compliance with the notice requirements.

There would be practical problems as well. If a consumer may orally waive the right to get notice until a later date, it will be difficult to police whether financial institutions are providing timely notice to all consumers because a financial institution could always claim that the consumer gave oral permission to receive the notice at a later date and it would be the institution's word against the consumer's word. Finally, how can a consumer make an educated decision to receive the notice at a subsequent time if the consumer doesn't yet know what that notice will say?

If the final rule allows a financial institution to provide the notice subsequent to establishing the customer relationship, we recommend the following:

- The Commission should require the financial institution to make an explicit oral disclosure that describes what the privacy notice would provide or that the financial institution read the privacy notice to the

consumer and that the written privacy notice be sent to the consumer no later than the next business day.

- Require the consumer/customer to subsequently document the oral waiver in writing and submit to the institution, which must maintain it on file.
- The financial institution should not be allowed to share information with nonaffiliated third parties until actual written notice is given to the customer and if the notice contains an opt out provision, the 30-day clock to opt out should not start running until the consumer receives actual written notice.

The Commission also solicited comments on who should receive notice in situations where there is more than one party to an account. We suggest the Commission add language to the rules to provide that all parties to an account must receive notice and an opportunity to opt out of information sharing with non-affiliates. As Regulation S-P recognizes in the definition of *non-public personal information*, the fact that an individual is a customer of a financial institution is protected by the GLBA provisions. It follows that all holders of an account are customers and deserve GLBA's protections, including notice.

INFORMATION TO BE INCLUDED IN INITIAL AND ANNUAL NOTICES OF PRIVACY POLICIES AND PRACTICES. (Section 248.6)

(a): General Rule.

(4) This provision requires the financial institution disclose the "categories of nonpublic personal information about former customers that [the financial institution intends to] disclose and the categories of affiliates and nonaffiliated third parties to whom [the financial institution intends to] disclose nonpublic personal information about [the financial institution's] former customers." In addition, footnote 42 of the Commission's release addresses opt out provisions for former customers. Neither the footnote nor the release, however, make clear that in order for a customer to exercise his or her right to opt out, the customer must, practically speaking, exercise such right before the customer ceases to be a customer, at which time the former customer will no longer receive notice of the right to opt out. Therefore, we recommend that the initial notice be required to be presented in a manner to put the a current customer on notice that failing to opt out will permit the financial institution to continue to share the individual's nonpublic personal information after the individual is no longer a customer. Inaction by a current customer will have ongoing consequences.

(d): Examples.

(3) Categories of affiliates and nonaffiliated third parties to whom you disclose. This provision is incorporated from GLBA and requires the disclosure of the "categories of affiliates and nonaffiliated third parties to whom the [financial institution] disclose[s] nonpublic personal information about [the financial institution's] consumers." GLBA leaves it to the regulators to define categories. We strongly support the

Commission's view that the notice specifically describe the categories of affiliates and nonaffiliates.

LIMITATION ON DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION ABOUT CONSUMERS TO NONAFFILIATED THIRD PARTIES (Section 248.7)

(a):

(3) Examples of reasonable opportunity to opt out. We suggest the Commission establish 30 days, from the issuance of the opt out notice to the consumer, as the minimum time period for a financial institution to provide for a consumer to opt out. Although a 30-day time period is suggested in the first example under this subsection, it could be viewed as only a suggestion and only apply to when the notice is provided to the consumer by mail. If a shorter time period is permitted, a consumer may be on vacation or business travel when the notice arrives and the consumer could be precluded from exercising his or her opportunity to opt out before any sharing of his or her personal information begins.

FORM AND METHOD OF PROVIDING OPT OUT NOTICE TO CONSUMERS. (Section 248.8)

(a):

(1) Form of opt out notice. We recommend the first sentence of this rule be amended to state explicitly that "a clear and conspicuous *written* notice" be provided to each consumer. Although subsection (b) "How to provide opt out notice", clearly states that the notice must be in writing and it may also be apparent from the wording of this subsection (a), this part of the rule should be clear on its face.

(2) Examples. As previously mentioned, we would recommend that the examples in this subsection be included in the rule as minimum standards of conduct under the rule. The consumer's awareness of the opt out opportunity is very important and directly related to the effectiveness of such notice. If the consumer does not observe the opt out notice and thus, does not exercise that right, the financial institution may begin to share the consumer's nonpublic personal information with nonaffiliated third parties. That consumer will not have another opportunity to observe the opt out notice until up to twelve months later. In the interim, the consumer's information can be shared.

(b):

(1) Delivery of notice. This subsection provides that if a consumer and a financial institution orally agree to enter into a customer relationship, the opt out notice may be provided to the customer within a reasonable time thereafter. We suggest that if a

financial institution wishes to disseminate a customer's nonpublic personal information to a non-affiliate when the customer relationship has begun under such circumstances, the opt out notice be attached to the initial notice and sent the next business day. We assume that in permitting the financial institutions to send an opt out notice subsequent to the establishment of a customer relationship, the financial institution would still be precluded from sharing the customer's data with non-affiliates until the customer receives notice and has a reasonable time to opt out.

(d) Continuing right to opt out.

We strongly support section 248.8(d) which provides that a "consumer may exercise the right to opt out at any time, and [the financial institution] must comply with the consumer's direction as soon as reasonably practicable." We believe that the last sentence of the last full paragraph of page 38 in the release should also be put into the rule reading "if a consumer elects to opt out of information sharing with nonaffiliated third parties, that election applies to all nonpublic personal information about that consumer in the financial institution's possession, regardless of when the information is obtained."

(e) Duration of consumer's opt out direction.

Paragraph 248.8(c) addresses how a firm can change the terms of its privacy policies and its obligation to provide a new opt out to allow dissemination of information to nonaffiliated third parties under the new policies. While we support the necessity of providing consumers with revised privacy policies and practices and requiring the financial institution to give notice to the consumer of the opportunity to opt out, we are concerned that if a consumer has exercised his or her right to opt out and the institution changes its policies, the consumer may be forced to continue to "watch the mail" for new notices and again exercise his or her right to opt out as to the new practice of the financial institution or permit the institution to share nonpublic personal information. We recommend the Commission make clear that this provision does not provide an institution another bite at the apple for a customer who has opted out. The result would burden the customer with having to opt out every time a firm changes its privacy policy.

OTHER EXCEPTIONS TO NOTICE AND OPT OUT REQUIREMENTS. (Section 248.11)

(a) Exceptions to opt out requirements.

(1) We strongly recommend that this provision be amended to state that the "consent" or "the direction" of the consumer be in writing. If this is not specified, confusion could occur regarding whether consent was given resulting in inappropriate sharing of information by the financial institution.

We congratulate the Commission on proposing rules addressing this very important subject of consumer privacy rights. If you have any questions about our comments, please do not hesitate to call me at (317) 232-6690 or Karen M. O'Brien, NASAA General Counsel at (202) 737-0900.

Sincerely,

Bradley W. Skolnik
Indiana Securities Commissioner
NASAA President