



March 31, 2000

Communications Division  
Office of the Comptroller of the Currency  
250 E Street, SW  
Washington, D.C. 20219  
Attention: Docket No. 00-05

Manager  
Dissemination Branch  
Information Management and Services Division  
Office of Thrift Supervision  
1700 G Street, NW 20552  
Attention: Docket No. 2000-13

Ms. Jennifer J. Johnson  
Secretary  
Board of Governors of the Federal Reserve  
System  
20<sup>th</sup> Street and Constitution Avenue, NW  
Washington, DC 20551  
Attention: Docket No. R-1058

Secretary  
Federal Trade Commission  
Room H-59  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Mr. Robert E. Feldman  
Executive Secretary  
Attention: Comments/OES (RIN 3064-AC32)  
Federal Deposit Insurance Corporation  
550 17<sup>th</sup> Street, NW  
Washington, D.C. 20429

Becky Baker  
Secretary of the Board  
National Credit Union Administration  
1775 Duke Street  
Alexandria, VA 22314

Jonathan G. Katz  
Secretary  
Securities and Exchange Commission  
250 5<sup>th</sup> Street, NW  
Washington, DC 20549  
File No. S7-6-00

**Re: Proposed Privacy Regulations**

Ladies and Gentlemen:

On behalf of members of the Consumer Bankers Association ("CBA"), this letter is submitted to the Office of the Comptroller of the Currency (the "OCC"), the Board of Governors of the Federal Reserve System (the "Board"), the Federal Deposit Insurance Corporation (the "FDIC"), the Office of Thrift Supervision (the "OTS"), the Federal Trade Commission (the "FTC"), the National Credit Union Administration (the "NCUA"), and the Securities and Exchange Commission (the "SEC") (collectively, the "Agencies") in response to the Agencies' request for comment on their Proposed Regulations concerning the Privacy of Consumer Financial Information (the "Proposed Regulations") issued pursuant to Title V of the Gramm-Leach-Bliley Financial Modernization Act (the "Modernization Act").

The Consumer Bankers Association is the recognized voice on retail banking issues in the nation's capital. Member institutions are leaders in privacy, consumer finance, student lending, retail delivery systems, small business services, and community development. CBA members include the nation's largest retail bank holding companies and hold two-thirds of the industry's total assets.

CBA acknowledges and appreciates the time and effort that the Agencies have expended to produce regulations that strive to balance the public policy concerns over the use of information with the

need for financial institutions to operate efficiently. We appreciate not only the efforts of the Agencies to issue the Proposed Regulations in such a short time frame but also the Agencies' recognition that uniformity in the rules is essential in the context of the Modernization bill.

As we grappled with the Proposed Regulations, working with different entities within the holding company structure, and representatives of the bank partners in this new information-based economy, our appreciation for the regulators' efforts on consistent guidelines increased enormously.

The complexity of the Final Rule will continue to be compounded by the changing face of the business world and technology advancements. As a result, we believe that it is important that the Agencies continue their joint efforts and that the industry and Agencies continue to work together on this issue.

CBA's Education Funding Committee comments are attached in Appendix A.

### **Issues of Principal Concern**

CBA members believe that, if the changes that stem from the Modernization Act are to prove beneficial to consumers and industry alike, the regulations—insofar as they may restrict the use of information—must be designed so as to encourage, not discourage, industry growth and participation in the evolving economy. To do this, the Final Rule must be both uniform and flexible.

#### **Uniformity Amongst the Rules**

Uniformity and consistency among the Rules governing the new financial institutions is paramount for consumers to realize the full benefits of a financial services holding company. The Act requires the Agencies to work together to assure “to the extent possible, that the regulations ... are consistent and comparable.” Congress recognized that uniformity would benefit industry and consumers alike. Particularly in the case of privacy, uniformity assures that consumers have similar privacy rights, without regard to the type of institution with whom they choose to do business. We are appreciative of the efforts that the Agencies have expended to achieve consistency and uniformity, and we would urge that the effort be continued, particularly in the definitions relevant to the institutions and information coverage of the Rules.

#### **Flexibility of Rules**

Flexibility is essential in the Final Rule in order to ensure consumer protection with a minimum compliance burden. Our specific comments below address a number of instances where we would encourage a greater flexibility. For one, the industry and consumers would both benefit from a longer implementation period to begin compliance with the Final Rule. An inflexible and overly short window to begin compliance, given the enormous operational and systems changes needed, will place unnecessary pressures on the institutions while causing implementation decisions to be based on the time pressures rather than the best interests of the customer. At the same time, the 30-day notice period would fall during the holiday season, during the busiest time of the year for mail, and the season of year-end disclosures and tax notices.

Flexibility is also needed in the content and timing of notices. For example, if the Regulations mandate overly detailed disclosures, the likelihood of “information overload” will only be increased.

Institutions need the flexibility to set the content to best meet the requirements in a manner that is meaningful to consumers. We also propose in our comments that greater flexibility be permitted in the timing of disclosure and the method of obtaining consent.

The following specific issues --addressed in more detail below-- are of paramount concern to CBA and its members:

- The effective date of the Final Rule
- The "clear and conspicuous" notice requirements
- The definition of "nonpublic personal information"
- The content of privacy notices
- The delivery of notice
- The restrictions on the use of account numbers

Following the discussion of these issues, we have provided additional comments on other matters, in the order they appear in the Proposed Regulations.

### **Effective Date**

The Proposed Regulations indicate a scheduled effective date of November 13, 2000. This six-month time frame does not provide the nation's financial institutions, and other companies affected by the rules, sufficient time to comply with the Modernization Act. The bill provides the most extensive regime of privacy regulations in the United States. Given the immense logistical requirements of implementing the regulations and the tremendous cost associated with implementation, requiring financial institutions to comply within the six-month period could easily result in imprudent implementation, significant additional expense, and unnecessary litigation.

All affected entities must: (1) develop and test a policy; (2) change new customer materials to reflect policy; (3) communicate policy to existing customers; and (4) finalize internal procedures to comply with other terms of new regulations. At each step, a myriad of internal and external changes must be made.

To demonstrate the enormous amount that must be accomplished between the issuance of the regulation and its implementation, we share the following list of implementation issues discussed at a recent CBA meeting:

### **Implementation of Privacy Regulations**

Define policy

- Determine corporate policy
- How can it be articulated simply, in terms that customers will readily understand?

## CBA Comment Letter

March 31, 2000

Page 4

- When a customer opts out, what does that mean to your company? How do you explain that?
- Can customers register different opt-out preferences in different businesses within your institution or will it be managed centrally?
  - How do you manage the customer preference database?
- Conduct research to understand your customers
- Where does the definition of privacy end, and data security begin?
- Test your message to ensure there are no unintended interpretations

### Develop disclosure

- How many versions? One is desirable, but may not be possible.
- Design communications questions
- What choices will you offer your customers?
- Test your communications pieces

### Business structure

- Does it make more sense to have each business line send disclosures to its own customers or to manage it centrally?
- How do you ensure consistency in customer communications and in implementation of customer preferences?

### Systems

- Do you have a system that can handle customer preferences or do you need to build a new one?
- What choices/preferences will you track?
- How will businesses and customer contact people know what each customer's preferences are?
  - Can you build business guidelines for customer interaction into the system instead of relying on training?
- Should each business keep track, or should it be tracked centrally?
  - How will you keep track if you don't have a central system?
- How will you handle customers who have multiple relationships?
- Collecting and aggregating information
  - What choices can you give to customers?
  - Where/how do you store it?
  - How to implement waiting period after disclosure and before sharing
  - How long to keep information after customer closes account

### How many individual customers do you have?

- With and without overlap of multiple accounts
- Is it sufficient to send one disclosure to a jointly held account?

### How will communication be done?

- Does it make more sense to send the disclosure in every statement, or to do a separate mailing to each individual customer?
- Statement stuffers?

- Lots of duplication means extra printing and postage – statements go first class, direct mail can go third class
- May be fairly heavy, due to volume of information required in disclosure
- Depending on weight and thickness, you may not even be able to statement stuff
- Likelihood of customers responding more than once drives up response handling costs
- Long lead time needed due to statement cycles
- Separate direct mail?
  - Could be aggregated by individual customer number (SSN, TIN or other)
  - One mailing to each customer instead of multiples
  - Can be sent with third class postage
  - Responses can be automatically scanned into system, reducing handling costs

#### Management of opt-out responses

- Estimate response rate, include contingency plans for possibility of higher rate of response
- Temporary increase in staff to record and acknowledge responses
- Training program for temporary staff

#### What response methodology will be used?

- 800 # IVR – could be programmed to allow customers to enter all their choices, but could have danger of overload at peak times, causing customer aggravation
- “Check off” form – would require customer to include own account number, would have to be manually keyed in to system, harder to process
- Scan-able form – most efficient handling method for back room, but would require separate direct mail methodology
- Customer writes letter – more work for the customer but most clear in terms of what customer really wants

#### How will responses be recorded?

- Can a customer opt-out once for the whole enterprise?
- Or will they opt-out separately for each affiliate?
- Determination of staffing needs for
  - Opening envelopes
  - Logging in preferences
  - Sending acknowledgement letters, formal process for escalation of customer complaints
  - Tracking and resolving problem responses
  - Answering telephone questions

#### How will responses be used?

- How do you make sure a customer's preferences are honored?
- How do business lines gain access to customer preference database?

#### Timeline

- When do you want to make your disclosures?

- Spread out over a few months or all at once?
- Right at the deadline when everybody else is bombarding customers with disclosures, or a little earlier?

#### Employee training

- Broad based training will be required for every customer contact employee
- Different information depending on need to know
- Employee access – how to limit appropriately, how to monitor

#### Audit

- Determine how to ensure consistent compliance

#### Communications

- Develop internal communications program to raise awareness, promote consistent responses from all employees
- Develop external communications (media, public policy) to promote consistent responses

The above list of issues -- substantial as it is -- is undoubtedly incomplete. Nevertheless, it demonstrates both the amount that must be accomplished and the considerable costs involved. The Agencies probably will be receiving individual cost estimates from different institutions as they comment on the Proposed Regulations, and we expect that they will be substantial.

The Agencies have proposed an effective date of November 13, 2000, the earliest date permitted by the Act. Because of these implementation demands, we respectfully request that the Agencies substantially delay the effective date. Although some have suggested an August 2001 implementation date, the complexity of the preparations, as well as the sheer number of companies and service providers that are affected, makes us concerned about even an August 2001 deadline. In fact, a number of banks, including those with experience in this area, believe that an extension as much as 18 months is called for. We encourage consideration of this request.

#### **Clear and Conspicuous**

The Proposed Regulations state that a notice is "clear and conspicuous" when it is "... reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice." We appreciate the Agencies' desire to provide guidance on the meaning of the term but we are concerned, however, that the proposed definition will have a number of adverse unintended consequences and, as discussed below, we urge the Agencies to either delete or modify the definition.

The most significant problem with the proposed definition of "clear and conspicuous" is that it is inconsistent with the FRB's longstanding interpretations of that phrase as it appears in several federal

consumer protection statutes. For example, under TILA, the FRB has interpreted "clear and conspicuous" in Regulation Z to mean that disclosures must be in a "REASONABLY understandable" form. The FRB has issued similar interpretations of clear and conspicuous under Regulations M, AA, CC and DD.

Congress was aware of these FRB interpretations when it chose to use the "clear and conspicuous" standard in the Modernization Act. Thus, we submit that Congress did not intend to give new meaning to the term "clear and conspicuous" without any statement to that effect in the Modernization Act or legislative history. As a result, we believe that any proposed definition of "clear and conspicuous" that varies from prior FRB interpretation is inconsistent with Congressional intent.

We also are concerned that the Agencies' attempt to set forth a different definition of "clear and conspicuous" under the Proposed Regulations will raise compliance questions regarding whether disclosures designed in reliance on the FRB's earlier interpretations of "clear and conspicuous" are deficient. The Proposed Regulations give no indication whether it is a clarification of the FRB's existing views or is a new definition of "clear and conspicuous." Many financial institutions may determine that it is necessary to significantly revise their existing disclosures under the Electronic Funds Transfer Act, TILA, the Truth in Savings Act, the Expedited Funds Availability Act and the Federal Trade Commission Act, to implement the Agencies' new definition. For these reasons, we urge the Agencies to delete the proposed definition of "clear and conspicuous" and instead, define the term to make it clear that compliance with the standard as previously articulated by the FRB will be deemed to comply with the standard set forth in the Modernization Act.

The Proposed Regulations provide examples of how a financial institution may comply with the "clear and conspicuous" standard. These examples set forth unusually specific guidance that would create significant uncertainty about how to comply. For instance, whether a particular disclosure is drafted in "clear, concise sentences," using "definite, concrete, everyday words," and avoiding "legal and highly technical business terminology" would invariably be subject to considerable debate and create enormous potential for litigation. In addition, each of these examples exacerbates the concerns stated above by magnifying the differences between the proposed definition and the longstanding FRB interpretations on which financial institutions have been relying for years.

We also note that paragraph (2)(iii) creates other concerns as well. It states that if a financial institution provides the Modernization Act notices on the same form as "another notice," the financial institution will be deemed to have designed its Modernization Act notice properly if it uses formatting such as "[l]arger type size(s), boldface or italics," or uses "[w]ider margins and line-spacing," or "[s]hading or sidelights to highlight the notice." This approach appears to suggest that the notices required under the Modernization Act are more important than other notices the consumer receives under other applicable federal law. We believe that, in view of the significance of many other disclosures required under the federal TILA and other similar statutes, it would be inappropriate to require more conspicuous disclosure of the Modernization Act requirements.

**Nonpublic Personal Information**

The Proposed Regulations set forth two alternative definitions of this term that are connected with the definitions of “personally identifiable financial information” and “publicly available information.”

Alternative A focuses on the source of the information and provides that information is public information only if it is actually obtained from a publicly available source. These sources include government records, widely distributed media, or government-mandated disclosures.

Alternative B, however, focuses on the information itself and where it is available. Therefore, information would be considered public information if it could be obtained from a publicly available source, even if it was obtained from a customer or other source.

We support adoption of Alternative B. The fact that information is available from a public source is more than sufficient to give that information the status of publicly available information regardless of how the financial institution obtained the information. To draft the Final Rule so as to make the treatment of information which is, in fact, available from a public source dependent on how the financial institution actually obtained it, is not practical and offers no additional safety measures for consumers.

We also agree that the term includes information from an Internet site that is available to the general public without requiring a password or similar restriction. We ask the Agencies to revise it to make it clear that the requirement to use a password to access a site does not in and of itself prevent a site from being available to the general public.

**Financial Information**

More significant, however, than the issues presented by Alternatives A and B is the meaning of the term “financial” for purposes of the regulation. This term is a critical component in the definition of nonpublic personal information. The Proposed Regulation’s interpretation of the term “financial information” is overly broad and is not supported by the statute or its legislative history. As explained in a colloquy between Senator Allard and Senator Gramm on Title V, Congress intended the term “personally identifiable financial information” only to include information that describes a consumer’s “financial condition.” Thus, the Final Rule should adopt the narrower definition of “financial information” intended by Congress—that is, only information that describes an individual’s “financial

condition,” such as an individual’s assets and liabilities, income, account balances, payment history and overdraft history.

There is little justification for broadening the definition of “personally identifiable financial information” to include information that is not financial in nature. In particular, the Final Rule should make clear that mere identification information, such as name, address and telephone number, is not “financial information” under the Final Rule. Similarly, the mere fact of a customer relationship, without any indication of the nature of the relationship (e.g., deposit account or credit card account), should not be considered “financial information” because it contains absolutely no information regarding the consumer’s “financial condition.”

### Content of Privacy Notices

CBA Holding Company members, if possible, would like to provide a common privacy notice to their customers, and appreciate the Proposed Regulation’s recognition that either common or separate notices can be given. The Proposed Regulations set forth examples of ways in which a financial institution may meet its Section 503 obligation to describe in its privacy notice: categories of information collected; categories of information disclosed; categories of nonaffiliated third parties to whom information is disclosed; disclosures of nonpublic personal information of former customers; and protecting the nonpublic personal information of customers.

However, the examples set forth in the Proposed Regulations would require a financial institution to include in the institution’s Section 503 privacy notice so much detail about the institution’s policies on collecting, disclosing, and protecting nonpublic personal information of consumers that such notices could not possibly be meaningful to most consumers. In fact, the Proposed Regulations, by requiring overly detailed privacy notices, would actually be counterproductive to the privacy interest of consumers. As a practical matter, a consumer is far less likely to read an institution’s privacy notice if it is lengthy and detailed.

In addition, by requiring overly detailed Section 503 privacy notices, the Proposed Regulations would impose substantial additional burdens on financial institutions, with no corresponding benefit to consumers. The extraordinary level of detail required by the Proposed Regulations could preclude affiliated financial institutions from providing consumers with a combined Section 503 privacy notice for those institutions.

We ask the Agencies to revise the examples, to reduce significantly the level of detail required for the Section 503 privacy notices, so that the Final Rule will help, rather than hinder, the understanding of the policy.

#### Security and Confidentiality

The Proposed Regulations call for financial institutions to describe their security policies and procedures in such detail that their effectiveness will be compromised. Security safeguards are constantly being addressed and improved for the benefit of the consumer and institution alike. Under the Proposed Regulations, financial institutions must re-disclose the security policy every time there are enhancements to these practices. This will create a large regulatory burden and serve as a disincentive to security advancements. The Final Rule should only require disclosing types of limitations on access of types or measures employed by the financial institution to protect information against reasonably anticipated threats or hazards.

#### Affiliates

We also note that the Proposed Regulations would establish initial and annual notice requirements that appear to be inconsistent with the plain language of the Modernization Act in two important respects. First, the Proposed Regulations states that the "categories of affiliates" to whom the financial institution discloses nonpublic personal information must be described in the initial and annual notices. We respectfully disagree. Section 503(a) provides a general description of the contents of the initial and annual disclosures. Section 503(a)(1) states that a financial institution must disclose its policies and practices with respect to "disclosing nonpublic personal information to affiliates and nonaffiliated third parties . . . including the categories of information that may be disclosed." Section 503(b), however, provides further explanation of "[t]he disclosure required by subsection (a)" and states that such disclosures shall include "the policies and practices of the institution with respect to disclosing nonpublic personal information to *nonaffiliated* third parties . . ." Moreover, Section 503(b)(1)(A) states that the disclosures made with respect to "*nonaffiliated* third parties" must include "the categories of persons to whom the information is or may be disclosed." The Modernization Act does not, at any point, state that the initial and/or annual disclosure must include any description of the categories of *affiliates* with whom a financial institution may share nonpublic personal information. The only reference in Section 503(b) to affiliate sharing is the specific statement that the initial and annual disclosures must include "the disclosures required, if any, under Section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act." Accordingly, any suggestion that the initial and/or annual notice must include the categories of affiliates is contrary to the plain language of the Modernization Act and, in our view, cannot be sustained.

Second, the Proposed Regulations appear to suggest that the initial and annual disclosures must describe information disclosed to all nonaffiliated third parties and must describe the categories of such third parties. The plain language of the Modernization Act, however, makes it clear that the initial and annual disclosures cover only those nonaffiliated third parties who are "other than agents of the [financial] institution." As a result, the Final Rule should clarify that information disclosed to third parties who are agents of the financial institution need not be described in the initial or annual disclosures. In addition, any such agents of the financial institution need not be described in the "categories of nonaffiliated third parties" to whom information is disclosed.

### **Delivery of Notice**

The Proposed Regulations provide that a financial institution must provide the initial notice to an individual "prior to the time" that the institution establishes a customer relationship with the individual. This requirement is inconsistent with the language in the Modernization Act which provides that a financial institution must provide the initial notice "at the time" of establishing a customer relationship.

If the agencies are concerned about consumers having "choice" in selecting a financial institution based on their privacy programs, we believe that other means can be used. For example, industry posts its privacy policies on the Web and should encourage consumers to review them. Any consumer can contact an institution regarding its privacy policies before becoming a customer. Policies can be made available upon request.

The Proposed Regulations recognize two situations (oral contracts and the purchase of portfolios) where additional flexibility is needed in regard to the initial notice. The Proposed Regulations would allow financial institutions, in these instances, to provide the initial notice within a reasonable time. Inevitably, there will be many other instances where it will be impossible or impractical for a financial institution to provide its initial privacy notice to a customer at the time of establishing a customer relationship. While most financial institutions will choose to provide the initial privacy notice with other required disclosures, the Final Rule should provide that a financial institution may deliver the initial privacy notice within a reasonable period after the customer relationship is established. This would only be permitted so long as no nonpublic personal information relating to that customer is disclosed to a nonaffiliated third party before the initial privacy notice and the opt-out notice are provided, and the customer is given a reasonable amount of time to opt-out before a disclosure can occur. This added flexibility will curtail undue hardships placed on financial institutions without sacrificing any privacy issues a customer may have.

### **Limits on Sharing of Account Numbers for Marketing Purposes**

#### Flat Prohibition

We believe that there are circumstances where a flat prohibition against disclosing account numbers, as provided in section 502(d) of the Modernization Act, might unintentionally disrupt certain

routine practices. For example, the prohibition would disrupt the disclosure of account numbers to a service provider who handles the preparation and distribution of monthly checking account statements for a financial institution coupled with a request by the institution that the service provider include literature with the statement about a product. The Proposed Regulations should make clear that the providing of account numbers by a financial institution to a service provider, agent or processor that is providing operational support for the financial institution, including marketing products on behalf of the financial institution itself, is not prohibited under Section 502(d) of the Modernization Act. In these instances, a service provider, agent or processor should be viewed as an extension of the financial institution itself, so in essence there is no "sharing" of information with a nonaffiliated third party.

#### Consent and Sharing Post Marketing

A consumer ought to be able to consent to the disclosure of his or her account number, notwithstanding the general prohibition in section 502(d) of the Modernization Act. The Proposed Regulations should be revised to specify that a financial institution may provide an account number to a nonaffiliated third party for use in marketing to the consumer, if the financial institution has obtained the consumer's prior consent. Also, the Proposed Regulations should make clear that Section 502(d) does not preclude a financial institution from providing an account number of a consumer to a nonaffiliated third-party after the consumer has already agreed to use the account to purchase the goods or services being offered. In these circumstances the account number is simply used to effectuate a transaction requested by a consumer after the marketing aspect has been completed.

#### Encrypted Account Numbers

An institution may not disclose an account number for marketing purposes to a nonaffiliated third party, other than to a consumer reporting agency. However, we believe that section 502(d) of the Modernization Act does not prohibit the disclosure by a financial institution to a non-affiliated third party for marketing purposes of encrypted account numbers if the financial institution does not provide the marketer the key to decrypt the number.

The Proposed Regulations should make clear that the term "account number or similar form of access number or access code" does not include (i) an actual account number or other number that can be used to post a charge or debit against a consumer's account, so long as that number is encrypted and the device or other information needed to decode or unscramble the encrypted number is not provided, and (ii) a reference number used by the financial institution to identify a particular account holder, including a partial or truncated account number, provided the reference number cannot be used to post a charge or debit against the particular account. Neither of these situations involves disclosure of an account number or similar form of access number or access code that a third party can use to directly post charges or debits to a customer's account.

### Other Issues

In addition to the issues presented above, CBA has comments on the following issues contained in the Proposed Regulations.

#### **Purpose and Scope (Section \_\_\_\_ .1)**

##### Foreign Financial Institutions

The Proposed Regulations indicate that it would apply to domestic offices of U.S. banks and domestic branches and Agencies of foreign banks. We support this provision and agree that the Proposed Regulations should not apply to foreign financial institutions that solicit business in the U.S., but do not have an office in the U.S. The Proposed Regulations should apply only to institutions with offices in the U.S. because enforcement mechanisms would not exist for foreign domiciled institutions.

#### **Rules of Construction (Section \_\_\_\_ .2)**

The Agencies have requested comment on whether including examples in the Final Rule will be useful. We believe that including examples is helpful, and we urge that the Agencies continue to provide examples in the Final Rule. We will recommend, however, changes to the examples included in the Proposed Regulations.

Section \_\_\_\_ .2 of the Proposed Regulations sets forth the "Rule of Construction" applicable to the proposed examples and specifically states that: (i) the examples are not exclusive; and, with the exception of the SEC version, (ii) compliance with an example constitutes compliance with the Rule. This Rule of Construction is an important clarification, and we urge that it be retained in the Final Rule.

#### **Definitions (Section \_\_\_\_ .3)**

##### Collect

The Proposed Regulations state that "[c]ollect means to obtain information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information." We ask the Agencies to consider two modifications to this definition. First, we urge that the Agencies clarify that the definition does not apply where an entity receives information and merely passes it along to another without storing the information itself. For example, when an entity receives a consumer credit application and simply transmits it to a financial institution for consideration, that entity should not be deemed to be "collecting" information provided that it does not retain information from the application. However, under the proposed definition, such an entity could be viewed as "collecting" the information because it "obtain[ed]" the information briefly. In order to address this issue, we recommend that the definition be modified to clarify that it applies only where an entity both obtains "and stores or maintains" the relevant information.

Second, we urge that the definition be modified to reflect the scope of the corresponding provisions of the Modernization Act more accurately. Specifically, we urge that the definition of "collect" be revised to state that it only applies to obtaining and storing or maintaining "nonpublic personal information." This would address the ambiguity created by the Proposed Regulations and accompanying Supplementary Information, which indicate that the definition would apply to obtaining "information," not just "nonpublic personal information."

#### Consumer

The Proposed Regulations' definitions and examples include as a "consumer" a person who submits a credit application to a financial institution. We believe the Proposed Regulations go beyond the provisions of the Modernization Act. The Proposed Regulations should be revised, consistent with the definition in the Modernization Act, to specify that an individual who merely submits an application or provides information to a financial institution, but does not actually obtain a products or services (such as a loan or account) from the financial institution, is not a "consumer" of the financial institution.

We urge the Agencies to replace the word "and" with "or" in this definition with respect to an individual's legal representative. An institution does not have a stand-alone relationship with a person's legal representative, but the definition appears to create two such relationships out of one. If applicable in a particular transaction, either the individual or the legal representative, but not both, ought to be considered a "consumer" and institutions should not issue multiple notices for a single relationship and should not have to deal at their peril with potentially conflicting instructions from the individual and the representative.

In the Proposed Regulations, a "customer relationship" requires a continuing relationship and the explanatory materials provide that repeated isolated transactions do not establish a customer relationship (e.g., periodic use of an institution's ATM machines, or repeated purchaser of traveler's checks or money orders). This point about isolated examples should be articulated directly in the examples in the Proposed Regulations by including the words, "or a series of isolated transactions" after the words "isolated transaction" in the first and third example. Furthermore, additional examples should be included in the Proposed Regulations for credit card advances and currency purchases.

#### **Initial Notice to Consumers of Privacy Policies and Practices Required (Section \_\_.4)**

#### Joint Accounts

The Agencies request comment on who should receive the initial Section 503 privacy notice in situations where there is more than one party to an account.

The Final Rule should permit an institution to provide the initial Section 503 privacy notice to only one party on the account. This position is entirely consistent with other consumer protection regulations, such as Regulation Z and Regulation E, which generally require that only one set of disclosures be sent to the parties to the account.

Requiring a financial institution to provide the notice to every party to the account would prevent financial institutions from coordinating the delivery of the initial Section 503 privacy notice with the disclosures required under other consumer protection laws.

If financial institutions are required to provide a copy of the initial Section 503 privacy notice to every party to the account, the institution would be forced to incur the enormous costs of establishing and implementing procedures for delivery of the initial Section 503 privacy notice to persons to whom the institution is not otherwise required to provide disclosures under other consumer protection laws, with multiple copies of the privacy notice often going to the very same address. For the most part, consumers would not benefit from the mandate, as the rule would substantially increase volume of disclosures consumers will receive under the Act, and increase the disclosure overload.

#### When the Financial Institution Establishes a Customer Relationship

We support the Agencies use of examples for this provision, but suggest that they be reformatted to indicate that the relationship is established when the bank rather than the consumer takes specified actions, such as provides credit, receives a deposit, etc. The mere execution of a form agreement by the consumer (whether or not part of the application process) should not be deemed to create any continuing relationship.

#### How to Provide Notice

The Proposed Regulations state that a financial institution must provide the initial privacy notice so that "each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form." We agree that the Modernization Act permits the delivery of notices in writing or electronic form. We are concerned, however, that the Proposed Regulations are attempting to establish a higher standard for the delivery of the Modernization Act disclosures than is found in other similar federal consumer protection statutes. Under the Modernization Act, a financial institution is required to "provide" certain disclosures to its consumers and customers. The Proposed Regulations, however, appear to suggest that a financial institution must determine whether the method for delivering a required disclosure to a consumer is such that the particular consumer "can reasonably be expected to receive actual notice." Although the examples set forth in the Proposed Regulations appear to suggest that typical methods of delivery may be acceptable, the general rule established by the Proposed Regulations suggests that it requires something more than merely "providing" the required disclosures. To avoid confusion on this point, we urge the Agencies to delete the standard it has created under the Proposed Regulations and instead more closely adhere to the language of the Modernization Act.

Specifically, we believe that the standard articulated by Congress in the Modernization Act can most clearly be articulated by stating in the Final Rule that required notices must be “delivered” or “provided” to consumers. Of course, each financial institution would be required to establish its own procedures to demonstrate that it has complied with the standard. We note that this approach would be consistent with the approach implemented by the FRB under other similar federal statutes [such as the TILA, EFTA and ECOA].

We commend the Agencies for acknowledging the permissibility of delivering the Modernization Act notices electronically. We urge the Agencies to modify the Proposed Regulations, however, to more closely track the requirements of the Modernization Act. In this regard, sections 502 and 503 of the Modernization Act both expressly state that the disclosures may be made “in writing or in electronic form.” These provisions do not impose different requirements on the two forms of delivery. Instead, the Modernization Act clearly states that the notices may be delivered in either form and do not impose any requirement that the consumer “agree” to delivery in electronic form.

#### **Annual Notice to Customers Required. (Section \_\_.5)**

##### General Rule

The Proposed Regulations provide that the annual notice requirement contained in the Modernization Act requires financial institutions to provide the institution’s privacy policy then in effect at least once during any period of twelve consecutive months. We suggest that the Final Rule provide additional flexibility in meeting this requirement. The Securities and Exchange Commission (“SEC”), in other rules requiring annual disclosure, affords the flexibility of providing the notice once each calendar year, but no less frequently than 15 months apart. This alternative would allow financial institutions to avoid technical non-compliance that could result from potential irregularities in the calendar and billing cycle brought on by acquisitions, divestitures or consolidations that are prevalent in the industry. We therefore propose that the Final Rule incorporate this same standard.

The Proposed Regulations provide that if a financial institution and a consumer orally agree to enter into a customer relationship, the institution may provide the opt-out notice within a reasonable time thereafter if the consumer agrees. There is no need for the Agencies to provide a more specific time by which the notice must be given. Institutions should be allowed to provide the opt-out notice to a consumer at any time before nonpublic personal information of the consumer is shared, provided the consumer is given a reasonable amount of time to opt-out.

The Proposed Regulations set forth examples of the circumstances under which a financial institution will be deemed to no longer have a continuing relationship with an individual. With respect to

a deposit account, the Proposed Regulations state that there is no continuing relationship with the account holder if the account is "dormant" under the financial institution's policies. We agree with the general intent of this interpretation, and we urge that it be included in the Final Rule. However, we urge the Agencies to modify the example by replacing the word "dormant" with the word "inactive." We are concerned that if the word "dormant" is used, it will create unnecessary uncertainty in view of the complex state law issues that come into play with respect to the meaning of that word. We believe that the word "inactive" achieves the result intended by the Agencies without creating such confusion.

The Proposed Regulations note that "for other types of relationships" a "continuing relationship" will no longer be deemed to exist where the financial institution "has not communicated with the consumer **about the relationship** for a period of 12 consecutive months, other than to provide annual notices of privacy policies and practices." This helpful clarification should be expanded to cover any type of customer relationship including a deposit account, closed-end loan, or open-end credit relationship such as those described in the earlier examples. Marketing materials may be frequently sent to customers as well as non-customers, and the fact that marketing materials are delivered to an individual is not relevant to the determination of whether there is a continuing relationship.

#### **Information to be Included in Initial and Annual Notices of Privacy Policies and Practices (Section \_\_\_ .6)**

##### Categories of Information Collected

The Proposed Regulations focus on the source of the information rather than the content of the information. The Proposed Regulations should be revised to provide greater flexibility by enabling institutions to comply by giving examples of the categories and allowing a financial institution to categorize information collected by source, by content or by a combination of both.

##### Categories of Information Disclosed

The Proposed Regulations focus on the content of the information. The Proposed Regulations should be revised to provide that a financial institution may give examples of categories and may categorize information disclosed by source, by content or by a combination of both. Also, there should be a recognition that broad categories or examples are acceptable and that not every element of information needs to be referenced.

**Limitation of Disclosure to Nonaffiliated Third Parties [Section \_\_\_\_ .7]**

The Proposed Regulations state that 30 days would be a reasonable period of time for a customer to exercise the opportunity to opt-out. We believe 30 days is ample time for the customer to exercise his or her opt-out rights, and do not suggest any change to this time period.

We do believe, however, that there should be some indication in the Proposed Regulations, and similarly in the opt-out notice given to the customer, that the financial institution is entitled to a reasonable period of time to process the opt-out notices before the election to opt-out becomes effective, in the event that the customer does not immediately elect to opt-out of the information sharing. A reasonable period of time is necessary to take into account manual entry of the information and to insure that the data reaches data warehousing systems. Although the Section-by Section Analysis of the Proposed Regulations indicates that "the financial institution would be permitted to disclose nonpublic personal information to nonaffiliated third parties for the period of time necessary to implement the consumer's opt-out direction," this same latitude is not found in the Proposed Regulations themselves. We believe it is important that the Final Rule indicate that there is some period of time involved in processing before the opt-out becomes effective, so that customers are not left with an expectation that an opt-out election will have immediate results.

**Form and Method of Providing Opt-out Notice [Section \_\_\_\_ .8]**

The Proposed Regulations state that a financial institution provides a reasonable means of opting out if it: (1) designates check-off boxes on the relevant forms with the Section 502 opt-out notice; (2) includes a reply form together with the opt-out notice; or (3) provides an electronic means to opt-out, if the consumer agrees to the electronic delivery of information. The Proposed Regulations, however, specify that a financial institution does not provide a reasonable means to opt-out by requiring consumers to send their own letter to the institution to exercise their right, although an institution may honor such a letter if received. We respectfully disagree with the statement in the Proposed Regulations that a financial institution does not provide a reasonable method of opting out if the consumer must write a letter to do so. There is nothing in the plain language of the Modernization Act or its legislative history that suggests this is not a reasonable means of communicating with a financial institution. Just as importantly, in other contexts, such as the billing error provisions of the federal TILA, it is expressly acknowledged that a consumer may be required to write in order to preserve his or her rights. Accordingly, we urge that the Agencies specifically make it clear in the Final Rule that requesting that a consumer write a letter is a reasonable means of opting out.

The example of the use of a toll-free number, at the institution's option, for opt-out purposes should be included. There should be no requirement, however, that a toll-free number must be made available or that an institution be forced to accept opt-outs through particular means of communication. An institution should be able to designate the means through which the opt-out may be communicated to it.

#### Duration of a Consumer's Opt-Out

As noted in the Proposed Regulations, a consumer's opt-out is effective until revoked by the consumer in writing or in electronic form "if the consumer agrees." We urge two modifications to this provision. First, we urge that the provision be modified to clarify that a consumer may revoke the opt-out by any reasonable means specified by the financial institution, not just in writing or in electronic form. Second, the provision should be modified by deleting any suggestion that a consumer must "agree" to disclosures in electronic form.

#### **Exception to Opt-out Requirements for Service Providers and Joint Marketing [Section \_\_.9]**

CBA does not believe that the "fully disclose" and contract requirements set forth in Section 502(b)(2) of the Modernization Act apply to service providers. In addition, CBA believes that the Agencies have further extended the contractual provision beyond anything set forth in the Modernization Act by imposing a use limitation. Specifically, even if the confidentiality contract requirement applies to service providers, the requirement relates solely to the maintenance of confidentiality. The provisions of Section 503(c) regarding the limits on reuse pertain only to redisclosure and do not restrict other uses of the nonpublic personal information. Sections \_\_.9(a) and \_\_.12 inappropriately impose restrictions on use which are not provided for in the Modernization Act.

The Agencies specifically seek comment on whether the Final Rule should require a financial institution to take steps to assure itself that the product being jointly marketed and other participants in the joint marketing agreement do not present undue risks for the financial institution. We urge the Agencies to refrain from imposing any such requirements under the Final Rule.

#### **Exceptions to Notice and Opt-out Requirements for Processing and Servicing Transactions [Section \_\_.10]**

Exceptions for Processing Transactions. The Proposed Regulations provide that the provisions pertaining to the initial notice to consumers, the consumer's opt-out notice, the consumer's right to opt-out, and the service provider/joint marketing do not apply if the financial institution discloses nonpublic personal information in a limited number of circumstances. These include when the disclosure is necessary to "effect, administer, or enforce" a transaction requested or authorized by the consumer, to "service or process" a financial product or service requested or authorized by the consumer, to maintain or service the consumer's account with the financial institution or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity, or in connection with a proposed or actual securitization or similar transaction.

We urge that the Agencies revise these provisions to make them consistent with the plain language of the Modernization Act. Specifically, under Section 502(e) of the Modernization Act, exceptions are provided for disclosures that are made "in connection with" servicing, processing or maintaining financial products or services of a consumer. This language is important because it makes it clear that disclosures can be made under these exceptions even if those disclosures are not necessarily required to service, process or maintain the account so long as they are made "in connection with" such activities.

CBA respectfully requests the Agencies to clarify that the consumer need not have directly requested or authorized the service provider to provide the financial product or services; request to the service provider's principal should be sufficient. The clarification is necessary because where a financial institution provides services as an agent, the individual consumer will have a relationship with the principal but not with the servicer, and so without the clarification, the individual's request or authorization could be deemed to relate only to the principal and not to the servicer.

#### **Other Exceptions to Notice and Opt-out Requirements [Section \_\_.11]**

##### Consent

The Proposed Regulations provide an example of consent with respect to referring a loan customer to a nonaffiliated insurance company. We believe that there are situations where consent ought to be implied. For example, the Proposed Regulations should make clear that co-brand and affinity programs are subject to notice and consent (and/or other exceptions), rather than notice and opt-out. Thus, given the nature of the program, a consumer participating in co-brand or affinity programs should not be able to opt-out of sharing. If the Agencies disagree with this point and believe the consumer may later opt-out, the Agencies should acknowledge that the financial institution, as a matter of contract, should be able to terminate the account or shift the consumer to another account, since the sharing is an integral aspect of the co-brand or affinity program.

**Appendix A**  
**Supplementary Statement of the Consumer Bankers Association**  
**Education Funding Committee**

The CBA Education Funding Committee consists of 14 of the largest 15 lenders participating in the FFEL program. In 1999, these lenders made more than \$10 billion in FFEL loans to more than 2,500,000 students. In the entire FFEL program, more than \$22 billion in student loans were made to more than 5,250,000 borrowers.

All FFEL Loans Should be Exempted from the Rules

Members of the CBA Education Funding Committee are major participants in the Federal Family Education Loan (FFEL) program, a program administered and regulated by the U.S. Department of Education ("ED"). FFEL is subject to detailed regulations that make these loans different than any other type of consumer loan. Historically, Congress has recognized the unique nature of student loans and has exempted the program from some otherwise applicable federal financial services regulations, including the Truth in Lending Act (see 20 U.S.C. 1083). Consistent with the history of FFEL, CBA believes that the special characteristics of student loans justify an exemption from the privacy rules. Such an exemption is justified because modifying systems and business practices in order to comply with the rules will undermine the effectiveness of servicing and other aspects of the administration of FFEL loans while not providing student loan borrowers with commensurate benefits. Importantly, the complications to loan servicing and administration, and potential confusion to student loan borrowers, could contribute to an increase in delinquency and default rates, a scenario that results in increased costs to taxpayers and to lenders participating in the student loan programs.

Our detailed comments are as follows:

Effective Date: Need for a Voluntary Compliance Period

Federal Family Education Loans are subject to extensive regulation requiring complex loan servicing systems involving lenders, guaranty agencies, third party service providers, and schools. In order to implement the disclosure requirements called for under the proposed regulations, a voluntary compliance rule, at the earliest 2001, should be established for both notices to student loan borrowers as well as for implementation of an opt-out system. Without such a voluntary compliance period, it is questionable whether many providers of student loans will be able to comply with the rule.

Definition of "Financial Institution" as Applicable to Third Party Servicers

The use of third party servicers is common in the federal student lending program. To avoid duplicative notices to borrowers, the Final Rule should unambiguously state that where a financial institution outsources activities to a third party service provider where the third party service provider performs services on behalf of the institution in servicing the institution's customers, the financial institution's customers are not customers of the third party service provider. Given that the third party service provider is not performing services to individuals, but instead to the financial institution, no separate notices should be required of such third party service providers.

Section 503 Privacy Notices to Customers

The proposed rule permits two or more affiliated financial institutions to use a common initial privacy notice, provided that the notice is accurate for all recipients. This provision works well for student loans, where student loans may be serviced by an affiliate of the financial institution making the loans. CBA supports this provision and urges its inclusion in the Final Rule.

Similarly, the proposed rule permits an institution to establish different privacy policies and practices for different categories of consumers, customers, or products, provided that the privacy notice received by each consumer or customer is accurate. Though institutions may want to craft a single policy, flexibility is important and this provision should be included in the Final Rule.

Section 503 Privacy Notices—Timing . Section \_\_\_\_\_ .4(a)(1)

Section \_\_\_\_\_ .4(a)(1) provides that a financial institution must provide the initial notice to an individual prior to the institution establishing a customer relationship with the individual. In the case of student loans, this provision would conflict directly with a common practice. Many student loan borrowers apply for and receive a commitment for student loan before the lender is selected. Thus, under the proposed rule, a customer relationship could exist before the lender chosen would have the opportunity to delivery an initial notice.

Means of Opting Out. Section \_\_\_\_\_ .8(a)(2)(ii)

In order to provide student loan customers with effective means of exercising the right to opt-out of disclosures, the Final Rule should identify easily accessible means of opting out. At the same time, however, the Final Rule should also allow financial institutions to specify reasonable means of opting out so as to avoid unnecessary and costly redesign of servicing systems and training of personnel to accommodate opt-out requests that may prove relatively rare.

Third Party Service Providers and Joint Marketing. Section \_\_\_\_\_ .9

For many lenders' student loan services, third party marketing agents are used. The language of section \_\_\_\_\_ .9 provides for an exception from opt-out requirements, but not from notice requirements. This requirement will result in lengthy and complex initial and annual notices being sent to student loan borrowers. In CBA's view, these notices will provide no benefit to thee borrowers.

Importantly, in the case of third party marketing in student lending, the student loan product is indistinguishable in the eyes of the consumer. Disclosing information regarding the third party marketer is unnecessary in that it does not contribute to the consumer protections of the consumer of the student loan.

CBA recommends that Section \_\_\_\_\_ .9 be modified to make clear that it does not apply to disclosure of information to nonaffiliated third parties performing services on behalf of the financial institution.

Exceptions to Notice and Opt-out Requirements. Section \_\_\_\_\_ .11(a)

In recent years, student loans have been subject to dramatic improvements in customer satisfaction. Much of this progress results from customer satisfaction surveys and other communications with borrowers to gather information on students' needs and expectations. Importantly, Department of Education data suggests that higher quality service to student loan borrowers decreases delinquency and default rates, which results in lower federal costs to support the program. To assure a continuation of the valuable tool of customer satisfaction surveys, CBA suggests that the following exception be added to section \_\_\_\_\_ .11(a).

“For surveys of applicants and customers for customer satisfaction and service quality relating to educational loans.”

CBA supports inclusion in the Final Rule of provisions excepting from notice and opt-out requirements disclosures made with the consumer's consent or direction, disclosures made to resolve borrower complaints or disputes or to respond to inquiries, disclosure to consumer credit rating agencies, and reports to consumer reporting agencies under the Fair Credit Reporting Act. All of these exceptions are necessary to meet customer expectations relating to the administration of FFEL loans. Without these exceptions, CBA believes student loan servicing could be undermined in a way that could lead to an increase in delinquencies or defaults.

Limits on Sharing of Account Number. Section \_\_\_\_\_ .13

Most student loan providers send borrowers monthly statements using third party servicing organizations. As currently written, the proposed rule would appear to prohibit the inclusion of the borrower's account number on a monthly statement printed or mailed by a third party servicer if the statement also includes marketing materials. The final regulations should provide an exception to address this problem.

CBA believes that the privacy interests of student loan borrowers are protected in accordance with the intentions of Title V where a financial institution furnishes information to a third party with the account number encrypted. In the case of information so shared, the privacy interests of the consumer with regard to the account number are fully protected. CBA recommends that the Final Rule clarify that disclosures with the account number encrypted be specified as specifically permitted.

The Agencies seek comment on whether safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion. The Agencies indicate that such safeguards might include, for instance, a requirement that consent be written or that it be indicated on a separate line in a relevant document or on a distinct Web page. We oppose any such requirements. Additional safeguards are not needed. Written consent ought not be required, particularly since many consumers enjoy and expect the convenience of conducting transactions by telephone.

**Limits on Redisclosure and Reuse of Information [Section .12]**

The Agencies seek comment on whether the Final Rule should require a financial institution that discloses nonpublic personal information to a nonaffiliated third party to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of that information. While a financial institution may wish to retain the right to audit a service provider, it should not be required to audit the activities of such nonaffiliated third parties, other than to contractually limit redisclosure of the information and enforce those contractual provisions should evidence of a violation arise. A financial institution could not effectively audit each third party to which it might disclose nonpublic personal information to ensure that such parties are complying with their statutory obligations to limit redisclosure of that information, but could enforce contractual obligations should violations occur. In addition, the Agencies retain the authority to review practices of entities acting as service providers to the financial institutions they supervise.

Thank you for your consideration of our concerns. Please feel free to call me at (703) 276-3873 if you have any questions or if I can be of assistance.

Sincerely,

A handwritten signature in cursive script that reads "Marcia Z. Sullivan". The signature is written in dark ink and is positioned below the word "Sincerely,".

Marcia Z. Sullivan  
Director, Government Relations

Attachment