

RUSSELL W. SCHRADER  
*Senior Vice President and  
Assistant General Counsel*



March 15, 2000

By Messenger

Jennifer J. Johnson  
Secretary  
Board of Governors of the  
Federal Reserve System  
20th and C Streets, NW  
Washington, DC 20551  
Docket No. R-1058

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

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

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

Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Jonathan G. Katz  
Secretary  
Securities and Exchange  
Commission  
450 5th Street, NW  
Washington, DC 20549  
File No. S7-6-00

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

Re: Proposed Privacy Regulations

Dear Sirs and Madams:

This letter is submitted in response to the request for comment from the Federal Reserve Board ("FRB"), the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC") and the Office of Thrift Supervision ("OTS") (collectively, the "Agencies") on their proposed privacy regulations ("Joint

VISA U.S.A. INC. Phone 650 432 3111  
Post Office Box 8999 Fax 650 432 2145  
San Francisco, CA 94128-8999  
U.S.A.

March 15, 2000

Notice”) implementing Title V of the Gramm-Leach-Bliley Act (“GLB Act”). We will refer to the proposed privacy regulations of the Agencies collectively as the “Proposed Rule.” In addition, this letter is submitted to the Federal Trade Commission (“FTC”) in response to its request for comment on the FTC’s proposed privacy regulations. Moreover, although this letter does not contain specific additional comments on the version of the privacy regulations proposed by the Securities and Exchange Commission (“SEC”) and the National Credit Union Administration (“NCUA”), we are submitting this letter to the SEC and the NCUA because their proposed privacy regulations present many of the same issues as the Agencies’ proposals. The comments set forth in this letter address a number of the issues raised in the Proposed Rule. Visa appreciates the opportunity to comment on this very important matter.

The Visa Payment System, of which Visa U.S.A.<sup>1</sup> is a part, is the largest consumer payment system in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies to benefit its 21,000 member financial institutions and their millions of cardholders worldwide. In fact, there are more than 970 million Visa-branded cards held by consumers globally, which generate over \$1.5 trillion in annual volume worldwide and over \$700 billion per year in the U.S. Visa is accepted at more than 18 million worldwide locations, including at more than 550,000 automated teller machines in the Visa Global ATM Network. Visa also has more than 80 smart card programs in 35 countries and on the Internet, with 23 million Visa chip cards, including over 8 million Visa Cash cards.

Visa applauds the federal regulators for working together to produce nearly consistent regulations among the federal agencies. It is critical that the final rules adopted by the agencies treat all financial institutions in a uniform manner, and, thus, we would urge that the remaining differences in the proposals also be rectified. As reflected in Section 504(a)(2) of the GLB Act, Congress clearly intended the federal agencies to work together to produce “consistent and comparable” privacy regulations among the agencies. In addition, uniformity of regulation benefits financial institutions and consumers alike. This uniformity is essential to maintaining and promoting competitive balance among entities in the financial services industry. Many diversified financial organizations have multiple regulators and all have business relationships with companies that will be regulated by the various agencies charged with regulating “financial institutions” as that term is defined in the GLB Act; the privacy rights of consumers, and the privacy obligations of financial institutions, should not change depending upon which primary regulator happens to regulate the particular financial institution. Uniformity in the privacy regulations will allow consumers to better comprehend their privacy rights under Title V of the GLB Act.

---

<sup>1</sup> Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

March 15, 2000

## **SUMMARY OF KEY COMMENTS**

In this letter, Visa provides comment on the many issues raised by the Proposed Rule. For convenience, we have organized our comments according to the Section number to which they relate. Nonetheless, in this summary, we will emphasize several of our most important points, with a reference to the page numbers containing the more detailed discussion.

### Timing of Effective Date.

The final Rule should provide that while the obligations of Sections 502 and 503 of the GLB Act and the implementing regulations become effective six months following the adoption of the final Rule, compliance with these obligations is voluntary until 12 months after the effective date (*i.e.*, until November 13, 2001). Sections 502 and 503 of the GLB Act place numerous new obligations on financial institutions. Indeed, financial institutions will not know the full extent of the obligations imposed under Sections 502 and 503 until the final Rule is released. Thereafter, financial institutions need adequate time to implement operational changes which are necessary to comply with these many new obligations. Requiring financial institutions to complete hastily all of the enormous system and operational changes within six months of when the final Rule is released would almost ensure mistakes on the part of financial institutions, to the detriment of institutions and consumers alike.

Although this voluntary compliance rule should apply to both new and existing customers of financial institutions, it is absolutely critical that the final Rule at least adopt a voluntary compliance rule of 12 months with respect to existing customers of financial institutions. For existing customers, the Proposed Rule provides that financial institutions are required to provide the Section 503 privacy notices within 30 days of the effective date of the regulations. This 30-day transition period is simply too short a time frame for financial institutions to provide Section 503 privacy notices to all of their existing customers, with many of whom they do not regularly correspond. Also, financial institutions would be required to provide these Section 503 privacy notices during the holiday season -- one of the busiest times for mail during the year. Financial institutions are already overburdened at this time of year preparing to send other special year-end disclosures to consumers -- such as notices for tax purposes. The short 30-day transition period also would place tremendous pressure on financial institutions in finding third-party servicing organizations to print these notices and provide them to consumers on behalf of the institutions. A voluntary compliance rule of 12 months would provide financial institutions with the flexibility they need to develop successfully their Sections 502 and 503 notices and to provide accurate notices to all of their existing customers. [See page 42 for more detailed discussion.]

March 15, 2000

Treatment of Agents, Processors and Service Providers in Section \_\_\_\_9.

Section \_\_\_\_9, as currently drafted, would have a disastrous effect on financial institutions, especially smaller institutions. In crafting the disclosure and opt-out provisions of Title V of the GLB Act, Congress intended to add wide-ranging consumer privacy protections without interfering with longstanding, essential outsourcing practices of banks and other financial institutions. Thus, Congress exempted various common servicing activities in two separate places: in Section 502(b)(2) and in Section 502(e). The combination of these two provisions was intended to allow a financial institution to continue to outsource to agents, processors, or other service providers *any* of the activities that the financial institution could perform itself. In drafting the proposed implementing regulations, however, the Agencies have inappropriately applied the disclosure and confidentiality requirements of Section 502(b)(2), intended for joint financial institution marketing arrangements, to traditional bank outsourcing arrangements, unless those outsourcing arrangements also qualify under Section 502(e). The failure to correct this inappropriate treatment of outsourcing arrangements would create substantial costs and operational problems for financial institutions, especially smaller institutions, with absolutely no corresponding benefits for consumers.

More specifically, under Section \_\_\_\_9 of the Proposed Rule, a financial institution would be required to include in its privacy policy disclosures, for most of its existing outsourcing arrangements, a separate description of the categories of information that are disclosed and the categories of third parties providing the outsourced services. In addition, under Section \_\_\_\_8 as proposed, a financial institution cannot change its outsourcing arrangements -- at least as to the types of information disclosed or the types of third-party service providers utilized-- unless and until the institution sends a change-in-terms notice to *all* of its customers. Such a misguided rule would be very costly for large banks who are members of bank holding companies, but at least they may have the option of using an affiliate for some of their outsourcing needs. But, for smaller institutions, such a requirement would be a disaster, because any cost savings that might be gained by a possible outsourcing arrangement would be eliminated by the costs of preparing, printing and mailing new privacy policy notices. The special disclosure and confidentiality requirements should be restricted to their intended application -- information shared between two or more financial institutions in connection with a joint marketing arrangement involving those nonaffiliated financial institutions. [See page 33 for more detailed discussion.]

Joint Accounts.

The final Rule should make it clear that if there is more than one party to an account, a financial institution is required to provide only one copy of the initial Section 503 privacy notice to the parties at the address specified by the parties for the account, or to the individual personally present at the institution or otherwise initiating the new customer relationship. Similarly, where the relationship requires an annual privacy notice, only one such notice should be required and that notice should be provided to the address specified for the relationship. This clarification is entirely consistent with other

March 15, 2000

federal 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. Likewise, a financial institution should be required only to provide the Section 502 opt-out notice to one party to the account.

Similarly, even where a financial institution provides the Section 502 opt-out notice to one party to the account, the financial institution should be prepared to honor an opt out from any party to the account. Nonetheless, the final Rule should provide flexibility to financial institutions with respect to how opt-out notices are provided to, and received from, the parties to a joint account. For example, *if* a financial institution is willing and has the operational capability to do so, it should be allowed to give joint account customers the opportunity to exercise different options, so that one customer might elect to have nonpublic personal information regarding that customer shared with third parties, while the other customer elects to opt out of such sharing. [See pages 19, 28 for more detailed discussion.]

#### Content of Section 503 Privacy Notices.

The examples set forth in the Proposed Rule 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 would be difficult to produce and maintain in an accurate fashion, and would not be meaningful to consumers. In fact, the Proposed Rule, by requiring overly detailed privacy notices, actually would be counterproductive to the privacy interests of consumers, because a consumer is less likely to read an institution's privacy notice if it is too lengthy and detailed.

In addition, by requiring overly detailed Section 503 privacy notices, the Proposed Rule would impose substantial additional burdens on financial institutions, with absolutely no corresponding benefits for consumers. In particular, the excessive level of detail required by the Proposed Rule could require a financial institution to provide different notices for its various product lines rather than a single notice for the institution as a whole, with many if not most customers receiving multiple and differing notices from the same financial institution. Moreover, by requiring overly detailed Section 503 privacy notices, the Proposed Rule would greatly increase the frequency with which financial institutions must provide change-in-terms notices regarding their privacy policies to consumers. These frequent change-in-terms notices would create significant confusion on the part of consumers and would impose enormous costs on financial institutions. Also, because of the substantial costs of providing these change-in-terms notices, the Proposed Rule, as currently drafted, could stifle innovation with respect to financial products and services.

Thus, unless the Agencies revise the examples to reduce significantly the level of detail required for the Section 503 privacy notice under the final Rule, the Rule would have the unintended consequence of harming consumers and financial institutions alike. [See page 23 for more detailed discussion.]

March 15, 2000

Flexibility Regarding Providing Section 503 Privacy Notices to Customers.

In the Joint Notice, the Agencies appropriately indicate that the Proposed Rule does not prohibit affiliated financial institutions from using a common initial Section 503 privacy notice, so long as the notice is delivered in accordance with the Rule and is accurate for all recipients. In addition, the Agencies indicate that the Rule does not prohibit an institution from establishing different privacy policies and practices for different categories of consumers, customers or products, so long as each particular consumer or customer receives a notice that is accurate with respect to him or her. In addition to reducing the detail required to be provided in such privacy notices, as discussed above, these important clarifications should be retained in the final Rule, since they provide financial institutions with the flexibility they need in deciding how best to structure their privacy policy disclosures to meet the needs of their customers.

In addition, the Agencies should clarify that if a financial institution delivers its privacy notice when a customer enters into a relationship with that institution, the institution is not required to deliver an additional privacy notice when the customer later enters into another relationship with that institution, so long as the privacy notice previously provided to *that* customer includes all of the information required for the new customer relationship being created. This clarification would in no way lessen or compromise the privacy interests of customers. It simply would make it clear that a financial institution is not required to incur the unnecessary costs of providing a duplicate copy of the institution's initial Section 503 privacy notice to a customer who has already received a copy of the notice. [See page 20 for more detailed discussion.]

Timing of Section 503 Privacy Notices.

The Proposed Rule in Section \_\_\_\_4(a)(1) provides 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. However, this "prior to" standard is entirely inconsistent with the statutory language of Section 503 of the GLB Act, which clearly states that a financial institution is expected to provide the initial privacy notice to a customer "at the time of" establishing a customer relationship.

Nevertheless, we applaud the Agencies for providing financial institutions with the flexibility of providing their privacy notice at the same time a financial institution is required to give other required notices regarding the account (such as the "initial disclosures" required under the Truth in Lending Act). These various notice requirements serve similar purposes of conveying important information to consumers at the commencement of the relationship, and no information regarding the consumer can be disclosed to nonaffiliated third parties until the consumer is given the required privacy notice and the opportunity to opt out.

Although in most cases financial institutions will choose to provide the Section 503 privacy notice with other required disclosures, the final Rule should provide financial institutions additional flexibility regarding the timing of the initial privacy notice.

March 15, 2000

Financial institutions need this flexibility to address situations where it might be impossible or impractical to provide its initial privacy notice to a customer at the time of establishing a customer relationship. Specifically, the final Rule should provide that a financial institution may deliver the initial Section 503 privacy notice within a reasonable period after the customer relationship is established, 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 Section 502 opt-out notice are provided, and the customer is given a reasonable amount of time to opt out. The privacy interests of customers would be protected because no information relating to that customer may be disclosed to any nonaffiliated third party until the customer receives the written privacy notice and has a reasonable opportunity to opt out of such disclosure. [See page 17 for more detailed discussion.]

#### Customers v. Consumers.

Section \_\_.3(i)(2)(ii)(A) of the Proposed Rule clarifies that the term “customer” does not include an individual who merely engages in an “isolated transaction” with a financial institution, such as an individual who purchases a cashier’s check or traveler’s check or uses the institution’s ATM to access the consumer’s account held at another institution. Also, the Agencies explain that an individual is not a “customer” of a financial institution merely because the individual repeatedly engages in such “isolated transactions” with the institution (*e.g.*, periodic use of an institution’s ATMs, or repeated purchases of traveler’s checks or money orders).

This important clarification should be retained in the final Rule. This reading of the term “customer” is entirely consistent with the GLB Act, which clearly contemplates a distinction between the terms “customer” and “consumer.” In addition, requiring institutions to provide initial and annual privacy notices to individuals who merely engage in isolated transactions would impose enormous costs on financial institutions, while providing absolutely no benefits to consumers. For example, the imposition of such a requirement on ATM transactions would force financial institutions to incur the tremendous costs of reconfiguring all of their ATMs to provide the privacy notices to persons who merely use the ATMs. Because of these costs, financial institutions may be forced to stop servicing the customers of other institutions, or increase the fee for such services, to the detriment of consumers and financial institutions alike. Moreover, the Proposed Rule adequately protects the privacy interests of individuals who engage in isolated transactions. Because such individuals would be “consumers,” a financial institution could not share the nonpublic personal information regarding those individuals to nonaffiliated third parties, without providing them with a copy of the institution’s privacy notice and giving them the opportunity to opt out of such disclosures.

Nevertheless, the Proposed Rule clearly exceeds the scope of the GLB Act by applying the term “consumer” not only to individuals who obtain financial products or services from financial institutions (as specified by the Act), but also to individuals who only apply for such products or services. The final Rule should be revised so that it is consistent with the statutory language. [See page 11 for more detailed discussion.]

March 15, 2000

Reasonable Means to Opt Out.

The example in Section \_\_\_\_8(a)(2)(ii) of the Proposed Rule relating to opt-out methods should be revised to make it clear that the use of toll-free telephone numbers provides a reasonable means to opt out. In this regard, the FTC, in its proposed privacy regulations, provides that a financial institution may designate a toll-free telephone number as a means that consumers can use to opt out. Both consumers and financial institutions would benefit by allowing a financial institution to provide a toll-free telephone number as a means that consumers can use to opt out. Consumers can simply make a toll-free call to opt out, and financial institutions would have the flexibility they need in providing opt-out methods that meet their needs, as well as the needs of their customers.

In the Supplemental Information included with the FTC's proposed privacy regulations, the FTC requests comment on whether financial institutions should be required to accept opt outs through any means the institution has already established to communicate with consumers. The final Rule should make it clear that a financial institution is not required to accept opt outs through any means the institution has already established to communicate with consumers. Requiring a financial institution to do so would force the institution to incur the enormous costs of establishing and implementing procedures to train all employees who interact with consumers in any way to handle opt-out requests, and would increase the possibility that a consumer's opt-out choice will not be properly implemented. Such a requirement also could force financial institutions to curtail the methods in which consumers may communicate with the institution, to the detriment of consumers and financial institutions alike. [See page 31 for more detailed discussion.]

Consent Exception.

The final Rule should make it clear that financial institutions have flexibility with respect to the methods they use to obtain consent from a consumer. In this regard, the final Rule should not require that a consumer's consent be in writing or indicated on a separate line in a relevant document or on a distinct Web page. Instead, the final Rule should only require that the consent opportunity be presented to the consumer in a clear and conspicuous manner, regardless of whether that opportunity is provided to the consumer in writing or orally.

With respect to standards relating to the scope of consent, the Agencies, at most, should only require that the consent provision be specific in its terms, such that the consent provision identifies the particular purposes for which information will be disclosed and the types of information that will be disclosed. In particular, the consent provision should not be required to identify the nonaffiliated third party to whom the information will be disclosed, other than by type of business, since the third party could and often does change, and a specific identification requirement would impose change-in-terms notice requirements on the financial institution. This approach to the scope of the consent provision is consistent with the approach used under the Fair Credit Reporting

March 15, 2000

Act (“FCRA”). Conversely, to the extent the financial institution is able to identify the particular nonaffiliated third party to whom information will be disclosed, the financial institution should be permitted to describe more broadly the particular purposes for which information will be disclosed and the types of information that will be disclosed with that nonaffiliated third party because it is the identity of that third party that is the basis of the consumer’s consent. This is particularly important in co-brand and affinity programs, as described below. [See page 36 for more detailed discussion.]

#### Nonpublic Personal Information.

Under the Proposed Rule, the Agencies essentially treat *any personally identifiable information* of a consumer as “financial information” if it is obtained by a financial institution in connection with providing a financial product or service to the consumer. As a result, the Proposed Rule’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 only intended the term “personally identifiable financial information” to include information that describes a consumer’s “financial condition.”<sup>2</sup> 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.

In particular, 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.” Similarly, the final Rule should make it clear that mere identification information (*e.g.*, name, address and telephone number) is not “financial information” under the Rule. [See page 13 for more detailed discussion.]

#### Public Information.

Under Section 509(4)(B) of the GLB Act, “publicly available information” is expressly excluded from the definition of nonpublic personal information. Nevertheless, in the Joint Notice, the Agencies seek comment on two alternatives of the definition of “nonpublic personal information” which differ in their treatment of information available from public sources. Under Alternative A, information is public information only if it is *actually* obtained from a publicly available source (*i.e.*, government records, widely distributed media or government-mandated disclosures). On the other hand, under Alternative B, information is public information if it *can be* obtained from a publicly available source, even if it was obtained from a customer or other source.

The final Rule should adopt the concept expressed in Alternative B -- that is, information which otherwise is generally available public information should not become

---

<sup>2</sup> 145 Cong. Rec. S13,902-03 (daily ed. November 4, 1999)

March 15, 2000

nonpublic information merely because it is provided to a financial institution by a consumer or customer, or from some other third-party source. To do otherwise would elevate source over substance and foster factual disputes over the immediate origin of information which, by definition, is available to anyone and everyone. Congress intended to exclude from the Act's coverage "publicly available information." If Alternative A is adopted, however, this statutory exclusion would be rendered utterly meaningless, and financial institutions would have to incur the unnecessary costs of tracking and proving the actual source of information they hold. We urge adaptation of Alternative B. [See page 14 for more detailed discussion.]

\* \* \* \*

The following contains additional comments on the Proposed Rule, organized according to the Section number to which they relate.

## **SECTION \_\_\_\_ .2. RULE OF CONSTRUCTION.**

The Proposed Rule uses examples to provide guidance regarding how the privacy requirements would apply in specific situations. In the Joint Notice, the Agencies ask whether such examples are useful and should be included in the final version of the Rule. The Agencies' use of examples not only should be retained in the final Rule, but should be expanded. The use of examples provides invaluable guidance to financial institutions on how to comply with the obligations of the GLB Act. In addition, the Agencies should retain in the final Rule the statement that the examples are not intended to be exhaustive. This important statement makes clear that the examples set forth in the Rule are just that, examples of how a financial institution may comply with the Act's requirements. Also, the final Rule should continue to state that compliance with an example, to the extent applicable, constitutes compliance with the requirements of the Rule. The valuable guidance provided by the examples would be rendered meaningless, as a practical matter, without the assurance that compliance with the examples constitutes compliance with the Rule.

Although the Agencies include many of the same examples in each of their individual privacy regulations, in some cases the wording of the examples differ substantively between the Agencies' versions of the regulations. For example, each of the Agencies' regulations contains an example of how a financial institution may comply with the requirement of including in its privacy policy a statement regarding the categories of information disclosed. The FRB and OTS versions of this example state that an institution meets this requirement by including the sources of information along with a *few* illustrative examples of content. However, the OCC and FDIC versions of this example do not contain the word "few." There is no reason why there should be differences in the wording of the examples, and these arguably substantive differences undercut the Agencies' efforts to produce consistent and comparable regulations. Thus,

March 15, 2000

the Agencies should ensure in the final version of their regulations that the wording of the examples is consistent among the Agencies' regulations.

### **SECTION \_\_\_3. DEFINITIONS.**

#### Definition of "Consumer".

In Section \_\_\_3(e), the Proposed Rule defines the term "consumer" to include an individual who merely submits an application, a response form, or otherwise provides nonpublic personal information to a financial institution in connection with obtaining a loan or account, but never actually obtains a loan or account from the institution. By including such individuals, the Proposed Rule's definition of "consumer" is inconsistent with the GLB Act. Congress -- by defining the term "consumer" to mean an individual who "obtains" a financial product or service from a financial institution -- intended the term "consumer" to include only individuals who actually obtain a loan or account from the institution. To make the final Rule consistent with the GLB Act, the Rule should make clear that the term "consumer" does *not* include an individual who merely submits an application, a response form, or otherwise provides information to a financial institution in connection with obtaining a loan or account, but never actually obtains a financial product or service from the institution.

#### Definition of "Customer".

Under Section 503 of the GLB Act, a financial institution is required to provide its privacy policy notice ("privacy notice") to its "customers" at the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship. In Section \_\_\_3(i), the Proposed Rule makes it clear that to be a "customer" an individual must have a continuing relationship with a financial institution. Thus, Section \_\_\_3(i)(2)(ii)(A) confirms that the term "customer" does not include an individual who merely engages in an "isolated transaction" with a financial institution, such as an individual who purchases a cashier's check or traveler's check or uses the institution's ATM to access the consumer's account held at another institution. Also, the Agencies explain that an individual is not a "customer" of a financial institution merely because the individual repeatedly engages in such "isolated transactions" with the institution (*e.g.*, periodic use of an institution's ATMs, or repeated purchases of traveler's checks or money orders).

This reading of the term "customer" should be retained in the final Rule, because it is entirely consistent with the GLB Act, which clearly contemplates a distinction between the terms "customer" and "consumer." More specifically, the term "consumer" is defined in the GLB Act as an individual who obtains a loan, account or other financial service or product primarily for personal, family or household purposes. Thus, the term "consumer" includes both individuals who have an ongoing relationship with a financial institution (defined as "customers"), as well as individuals who merely engage in isolated

March 15, 2000

transactions with the institution. If the term “customer” is read broadly to include individuals who engage in isolated transactions with a financial institution, the term “customer” and the term “consumer” would be synonymous, and the distinction between the terms intended in the statute would disappear.

In addition, individuals who engage in isolated transactions with a financial institution are not “customers” of that institution in any real sense. For example, in ATM and check-cashing transactions, an individual’s banking relationship is with the financial institution that holds the individual’s deposit account, and under the statute the individual will receive a privacy policy from that institution. Requiring institutions to provide initial and annual privacy notices to individuals who merely engage in isolated transactions would impose enormous costs on the institutions, while providing absolutely no benefits to consumers. For example, the imposition of such a requirement on ATM transactions would force financial institutions to incur the tremendous costs of reconfiguring all of their ATMs to provide the privacy notices to persons who merely use the ATMs. Because of these costs, financial institutions may be forced to stop servicing the customers of other institutions, or increase the fee for such services, to the detriment of consumers and financial institutions alike.

Also, requiring a financial institution to provide its annual privacy notice to individuals who merely engage in isolated transactions would actually force the institution to collect and retain more information regarding such individuals than the institution would otherwise have collected and retained with respect to such transactions. This result would be entirely inconsistent with the privacy purposes of the GLB Act. For example, if an institution were required to provide an annual privacy notice to individuals who engage in check-cashing transactions, the institution would, at a minimum, be required to collect and retain the individual’s name and address, so that the institution could provide the individual with that annual notice.

Moreover, the Proposed Rule adequately protects the privacy interests of individuals who engage in isolated transactions. Because such individuals would be “consumers,” a financial institution could not share the nonpublic personal information regarding those individuals with nonaffiliated third parties, without providing them with a copy of the institution’s privacy notice and giving them the opportunity to opt out of such disclosures.

For all of these reasons, the important confirmation that an individual who merely engages in isolated transactions with a financial institution is not a “customer” of the institution for purposes of Section 503 should be retained in the final Rule.

#### Definition of “Financial Institution”.

In the Supplemental Information to the FTC’s proposed privacy regulation, the FTC indicates that many entities that come within the broad definition of financial institution will likely not be subject to the disclosure requirements of the Rule because not all financial institutions have “consumers” or establish “customer relationships.” For

March 15, 2000

example, the FTC indicates in the Supplemental Information to its proposal that courier services and data processors who perform services for a financial institution, but do not themselves provide financial products or services to individuals, will not be required to make the disclosures mandated by the Rule because they do not have “consumers” or “customers” as defined by the Rule.

This is an important clarification that should be incorporated into the final Rule. In particular, the final Rule should make clear that when a financial institution outsources activities to an agent, processor or other third-party service provider where the agent, processor or third-party service provider performs services on behalf of the institution in servicing the institution’s customers or consumers, the institution’s consumers or customers are not considered “consumers” or “customers” of the agent, processor or third party service provider. In this regard, these agents, processors or third-party service providers are not providing any “financial products or services” directly to individuals, but instead are providing the services to the financial institution, and requiring such service providers to provide privacy notices would greatly increase the costs of such outsourcing arrangements for institutions, and thus for consumers, with no corresponding consumer benefits.

For example, financial institutions will often outsource activities to a third-party service provider in processing ATM and point-of-sale debit and credit card transactions on behalf of the institution, and the third-party service provider is providing a service to the institution and not to the institution’s debit or credit cardholders. Thus, the institution’s cardholders should not be considered “consumers” or “customers” of the third-party service provider merely because the third-party service provider is providing services to the financial institution in processing the ATM or point-of-sale debit and credit card transactions.

#### Definition of “Nonpublic Personal Information”.

##### *Financial Information.*

Under Section 509(4) of the GLB Act, the term “nonpublic personal information” is defined to mean “personally identifiable financial information” that is provided by a consumer to a financial institution, results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. Under the Proposed Rule, however, the Agencies essentially treat *any personally identifiable information* of a consumer as “financial information” if it is obtained by a financial institution in connection with providing a financial product or service to the consumer.

As a result, the Proposed Rule’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 only intended the term “personally identifiable financial information” to include information

March 15, 2000

that describes a consumer's "financial condition."<sup>3</sup> 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.

In particular, 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." Similarly, the final Rule should make clear that mere identification information (*e.g.*, name, address and telephone number) is not "financial information" under the Rule.

*Publicly Available Information.*

Under Section 509(4)(B) of the GLB Act, "publicly available information" is expressly excluded from the definition of nonpublic personal information, and the Proposed Rule correctly defines "publicly available information" as any information that is lawfully made available to the general public from: (i) federal, state or local government records; (ii) widely distributed media; or (iii) disclosures to the general public that are required to be made by federal, state or local law. Nevertheless, in the Joint Notice, the Agencies seek comment on two alternatives of the definition of "nonpublic personal information" -- Alternative A and Alternative B -- which differ in their treatment of information available from public sources. Under Alternative A, information is public information only if it is *actually* obtained from a publicly available source (*i.e.*, government records, widely distributed media or government-mandated disclosures). On the other hand, under Alternative B, information is public information if it *can be* obtained from a publicly available source, even if it was obtained from a customer or other source.

The final Rule should adopt the concept expressed in Alternative B -- that is, information which otherwise is generally available public information should not become nonpublic information merely because it is provided to a financial institution by a consumer or customer, or from some other third-party source. To do otherwise would elevate source over substance and foster factual disputes over the immediate origin of information which, by definition, is available to anyone and everyone.

Congress intended to exclude from the Act's coverage "publicly available information." If Alternative A is adopted, however, this statutory exclusion would be rendered utterly meaningless, and financial institutions would have to incur the unnecessary costs of tracking and proving the actual source of information they hold. For example, under Alternative A, if a financial institution collected a consumer's name, address and telephone number from the consumer, the information would not be considered "publicly available information" because it was not actually collected from a public source, even though that same information is readily available to anyone from a

---

<sup>3</sup> 145 Cong. Rec. S13,902-03 (daily ed. November 4, 1999)

March 15, 2000

public source. In addition, in order for the financial institution to exclude the generally available name, address and telephone number from the Act's coverage, the institution would be forced to incur the costs of re-collecting that same information from a public source. And, even then, the financial institution would be required to establish costly procedures to prove that the information was collected from a public source.

In addition, in many cases, a financial institution simply may not know the source of the information it holds. For example, when a financial institution buys a portfolio of accounts, the institution may not have the information necessary to determine whether information associated with those accounts actually was obtained from a public source. All it will know is that the information can be obtained from a public source and, thus, that the consumer cannot possibly expect that such publicly available information would be treated as if it were nonpublic information. For all of these reasons, if Alternative A were adopted, the final Rule would vitiate the intent of Congress to exclude "publicly available information" from the definition of "nonpublic personal information." We urge adaptation of Alternative B.

The FTC, in its proposed privacy regulations, invites comment on whether a variation of Alternative A or Alternative B should be adopted that would require a financial institution to undertake reasonable procedures to establish that information is, in fact, available from public sources before the financial institution may disclose it without restriction as "publicly available information." Requiring financial institutions in each and every case to verify that information is actually publicly available before the institution may disclose it as "publicly available information" would impose significant costs on financial institutions, without any corresponding benefits to consumers. For certain types of information, which ordinarily is publicly available, such as information usually contained in public records, financial institutions should be allowed to assume that such information is publicly available, without being forced to incur unnecessary costs in verifying in each instance that such information is actually publicly available. Thus, the Agencies should make it clear that financial institutions can assume, for example, that such public records as title transfers for home sales and related purchase amounts is publicly available information, without being forced to incur the unnecessary costs of verifying on a case-by-case basis for each particular consumer that such typically public information is actually publicly available.

#### *Depersonalized Information.*

In the Joint Notice, the Agencies also invite comment on whether the term "nonpublic personal information" should cover information about a consumer that contains no indicators of a consumer's identity when it is communicated to a nonaffiliated third-party recipient (so-called "depersonalized information"). Under Section 509 of the GLB Act, the term "nonpublic personal information" only includes "personally identifiable financial information." By using the term "personally identifiable," Congress clearly intended to exclude information that contains no indicators of a consumer's identity *when communicated to a nonaffiliated third-party recipient*. Also, there is absolutely no policy rationale for including depersonalized

March 15, 2000

information in the term “nonpublic personal information.” The GLB Act is designed to protect a consumer’s privacy interest with respect to the consumer’s financial information. A consumer’s privacy cannot be compromised by disclosing depersonalized information, because that information, by definition, does not identify any individual consumer.

Financial institutions use depersonalized information in connection with market studies, and for financial modeling and to develop score cards for evaluating applications for both credit and deposit products. For example, a mortgage lender often provides depersonalized aggregate information about its mortgage loans for the purpose of preparing market studies. These market studies provide invaluable information to both consumers and financial institutions alike, in helping them to understand trends in the lending markets. Restricting the use of depersonalized information would fundamentally change the way financial institutions do business, and would undermine the safety and soundness of such institutions. Thus, it is imperative that the final Rule make it clear that depersonalized information is not included within the definition of “nonpublic personal information.”

*Widely Distributed Media.*

The Agencies also seek comment on what information is appropriately considered publicly available, particularly in the context of information available over the Internet. In this regard, the Proposed Rule defines the term “publicly available information” to include information from an Internet site that is available to the general public without requiring a password or similar restriction. The Proposed Rule appropriately treats the Internet as a widely distributed medium. In fact, the Internet is the epitome of “widely distributed media” because people all over the world have access to information made generally available through the Internet.

With respect to the requirement relating to “password or similar restriction,” the Agencies should make clear that this requirement does not include an access fee or logon password that an individual ordinarily is required to provide to an Internet service provider in order to use the Internet service provider’s service. If such access fees or logon passwords were read to be included within the phrase “password or similar restriction,” then almost none of the useful information that is widely available over the Internet would be considered “publicly available information.” Thus, a broad reading of the term “password or similar restriction” to include such system or portal access fees or logon passwords would defeat the whole purpose of including the Internet as a widely distributed medium.

**SECTION \_\_\_ .4. INITIAL NOTICE TO CONSUMERS OF PRIVACY POLICIES AND PRACTICES REQUIRED.**

Timing of the Initial Section 503 Privacy Notice to Customers.

March 15, 2000

The Proposed Rule in Section \_\_\_\_4(a)(1) provides 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. However, this “prior to” standard is entirely inconsistent with the statutory language of Section 503 of the GLB Act, which clearly states that a financial institution is expected to provide the initial privacy notice to a customer “at the time of” establishing a customer relationship. While most financial institutions may elect to make their privacy policies known to both customers and prospective customers on their Web site or by making disclosures or brochures available at branches and other public locations, the statutory requirement for providing the institution’s privacy notice clearly is “at the time of” establishing a customer relationship, rather than some undefined point “prior to the time” that relationship is established. In this regard, as most banks and other financial institutions have already followed the recommendations of the Agencies to post their privacy notices on the institution’s Web site and, thus, any perceived need for financial institutions to make their privacy notices generally available to prospective customers has already been addressed.

We applaud the Agencies, however, for providing financial institutions with the flexibility of providing their privacy notice at the same time a financial institution is required to give other required notices regarding the account (such as the “initial disclosures” required under the Truth in Lending Act). These various notice requirements serve similar purposes of conveying important information to consumers at the commencement of the relationship, and no information regarding the consumer can be disclosed to nonaffiliated third parties until the consumer is given the required notice and the opportunity to opt out.

This is a critically important clarification that should be retained in the final Rule. Both customers and financial institutions benefit by allowing financial institutions to combine the initial privacy notice with other required disclosures. Customers benefit by conveniently receiving important disclosures and notices regarding a loan or account at one time, instead of at scattered points during the process of establishing a customer relationship, and financial institutions benefit by not being forced to incur the substantial costs of establishing, instituting, and monitoring compliance with, procedures for the multiple delivery of disclosures to the same customer in connection with establishing the same loan or account. Requiring a financial institution to establish and implement separate delivery procedures would essentially double the costs that institutions face today in delivering required disclosures to customers, costs that ultimately will be passed on to customers.

Although in most cases financial institutions will choose to provide the Section 503 privacy notice with other required disclosures, the final Rule should provide financial institutions additional flexibility regarding the timing of the initial privacy notice. Financial institutions need this flexibility to address situations where it might be impossible or impractical to provide its initial privacy notice to a customer at the time of establishing a customer relationship. Specifically, the final Rule should provide that a financial institution may deliver the initial Section 503 privacy notice within a reasonable period after the customer relationship is established, so long as no nonpublic personal

March 15, 2000

information relating to that customer is disclosed to a nonaffiliated third party before the initial privacy notice and the Section 502 opt-out notice are provided, and the customer is given a reasonable amount of time to opt out before any such disclosure can occur.

In this regard, the Proposed Rule already recognizes two situations (oral contracts and purchases of portfolios) where it is not feasible for a financial institution to provide the initial Section 503 privacy notice to a customer at the time the customer relationship is established, but numerous other similar situations exist. For example, a financial institution may allow a consumer who opens a credit card account at the point of sale to immediately use that account to make a purchase. In these situations, it is often a third party, and not the financial institution itself, that accepts the application for the credit card account and forwards that information to the financial institution. It would be difficult for the institution to ensure that the third party has the most recent copy of the institution's privacy notice, and that the notice was actually given to the customer by the third party at the point of sale. In addition, it may be more convenient for the customer to receive the privacy notice at a later time, such as when the credit card itself is mailed to the customer or when a "welcome kit" regarding the account is mailed. Moreover, the customer's privacy interests would be protected because no information relating to that customer may be disclosed to any nonaffiliated third party until the customer receives the written privacy notice and has a reasonable opportunity to opt out of such disclosure.

The same need for flexibility also arises in the situation where a financial institution provides a mailed preapproved credit card solicitation to consumers and allows consumers who accept the preapproved solicitation to use the credit line available on the credit card immediately (such as for a balance transfer), before the credit card device is sent to the consumer. Requiring the institution to send its Section 503 privacy notice with each of the mailed preapproved credit card solicitations would impose enormous costs on financial institutions, without any benefits to consumers. Again, the customer's privacy interests would be protected in such circumstances because no information relating to that customer may be disclosed to any nonaffiliated third party until the customer receives the written Section 503 privacy notice and has a reasonable opportunity to opt out of such disclosure.

With respect to oral contracts, the Proposed Rule specifies that if a financial institution and a customer orally agree to enter into a customer relationship, the institution may provide the Section 503 privacy notice to the customer within a reasonable time thereafter *if the customer agrees*. This notion that a customer must agree to receive the Section 503 privacy notice at a later time is confusing and unnecessary and should be deleted. With respect to oral contracts, the financial institution has no alternative but to provide the written Section 503 privacy notice to the customer at a time after the customer relationship has been established orally because, under the Proposed Rule, the institution is not allowed to provide the Section 503 privacy notice orally to the customer. When a customer has already agreed orally to enter into a customer relationship with a financial institution, requiring the institution also to obtain the consent of the customer to receive the Section 503 privacy notice at a later time is unnecessary and could lead to customer confusion. Moreover, customers' privacy interests are

March 15, 2000

adequately protected in such circumstances because a financial institution is prohibited from disclosing information relating to that customer to any nonaffiliated third party until the customer receives the written Section 503 privacy notice and has a reasonable opportunity to opt out of such disclosure.

#### Joint Accounts.

In the Joint Notice, 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 make it clear that if there is more than one party to an account, a financial institution is required only to provide one copy of the initial Section 503 privacy notice to the parties at the address specified by the parties for the account, or to the individual personally present at the institution or who otherwise is the party who initiates the relationship on behalf of the joint account customers. This clarification 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 initial Section 503 privacy notice to every party to the account would eliminate the benefit to financial institutions of allowing them to coordinate the delivery of the initial Section 503 privacy notice with the disclosures required under other consumer protection laws. In particular, if financial institutions were 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 both copies of the privacy notice ordinarily going to the very same address.

#### How to Provide Notice.

In the Joint Notice, the Agencies appropriately indicate that the Proposed Rule does not prohibit affiliated financial institutions from using a common initial Section 503 privacy notice, so long as the notice is delivered in accordance with the Rule and is accurate for all recipients. In addition, the Agencies indicate that the Rule does not prohibit an institution from establishing different privacy policies and practices for different categories of consumers, customers or products, so long as each particular consumer or customer receives a notice that is accurate with respect to him or her. These important clarifications should be retained in the final Rule, since they provide financial institutions with the flexibility they need in deciding how best to structure their privacy policy disclosures to meet the needs of their customers.

March 15, 2000

In addition, the Agencies should clarify that if a financial institution delivers its privacy notice when a customer enters into a relationship with the institution, the institution is not required to deliver an additional privacy policy notice when the customer later enters into another relationship with the institution, so long as the privacy notice previously provided to *that* customer includes all of the information required for the new customer relationship being created. This clarification would in no way lessen or compromise the privacy interests of customers. It simply would make it clear that a financial institution is not required to incur the unnecessary costs of providing a duplicate copy of the institution's initial Section 503 privacy notice to a customer who has already received a copy of the notice.

#### Methods of Providing Notice.

The Proposed Rule indicates that a financial institution must provide its Section 503 privacy notice so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form. In the Joint Notice, the Agencies indicate that for consumers who have obtained a financial product or service from the institution electronically, electronic delivery of the initial Section 503 privacy notice generally should be in the form of electronic mail, although a Section 503 privacy notice on the Web site can be used, so long as the consumer is required to access the notice to obtain the product or service in question.

With respect to consumers who have agreed to receive information electronically from the institution, the final Rule should specify that a financial institution may satisfy its obligation to provide the initial and annual Section 503 privacy notice to such consumers, by simply posting the institution's Section 503 privacy notice on its Web site. Thus, a financial institution should not be required to send the initial or annual Section 503 privacy notice to such consumers via e-mail or require such consumers to access the Web site page on which the Section 503 privacy notice is posted in order to obtain the product or service in question.

Requiring a financial institution to provide its initial and annual Section 503 privacy notice to consumers via e-mail or through required access to the Web site page containing the Section 503 privacy notice, imposes unnecessary costs on the financial institution, with no accompanying benefits to consumers. By posting the Section 503 privacy notice on its Web site, a financial institution has provided consumers continual access to its Section 503 privacy notice. A financial institution should not be required to essentially "spam" consumers who have agreed to receive information electronically from the institution with unnecessary e-mails on either an initial or annual basis, when the consumer can access the institution's Web site at any time to obtain the institution's Section 503 privacy notice. Thus, the final Rule should provide that with respect to a consumer who has agreed to receive information electronically, a financial institution meets its obligation to provide an initial and annual Section 503 privacy notice to such consumer, by either posting its Section 503 privacy notice on its Web site or providing the notice via e-mail to the consumer.

March 15, 2000

Notice to Customers.

In the Joint Notice, the Agencies also request comment on whether and how the Proposed Rule should address situations where a customer has requested a financial institution not to send statements, notices or other communications to the customer. The final Rule should make clear that customers can essentially “opt out” of receiving the initial Section 503 privacy notice, the annual privacy notice and the Section 502 opt-out notice by opting out of receiving any communications from the institution. In this regard, the final Rule should not require a financial institution to alienate its customers by forcing the institution to provide notices to a customer where the customer has specifically instructed the institution not to communicate with the customer with respect to the account. In particular, the mailing of such a notice could violate the customer’s intended confidentiality regarding the very existence of that account.

Retention or Accessibility of Notice for Customers.

The Proposed Rule specifies that in the case of customers, the Section 503 privacy notice must be given in such a way that the customer may either retain it or access it at a later time. In this regard, the Agencies should make it clear that it is the financial institution that has the option to provide the Section 503 privacy notice by either (i) giving the notice in a form that a customer can retain, or (ii) allowing the customer to obtain another copy of the institution’s current privacy notice at a later time. In certain circumstances, such as in electronic transactions, it may difficult for financial institutions to provide the Section 503 privacy notice to a customer in a form that the customer can retain. Thus, it is critical that the final Rule provide financial institutions with the flexibility either to provide the Section 503 privacy notice in a form that the customer can retain or to allow the customer to obtain another copy of the institution’s *then current* privacy notice at a later time.

**SECTION \_\_\_\_.5. ANNUAL NOTICE TO CUSTOMERS.**

The Proposed Rule states that a financial institution is not required to send the Section 503 privacy notice annually to a customer with whom it no longer has a continuing relationship. Additionally, the Proposed Rule sets forth examples of when there is no longer a continuing relationship, such as: (1) deposit accounts that are dormant under the institution’s policies; (2) closed-end accounts that have been paid in full, charged off or sold without the institution retaining servicing rights; (3) open-end credit accounts where periodic statements are no longer sent or where such accounts are sold without the institution retaining servicing rights; and (4) other types of accounts, where the institution has not communicated with the customer about the relationship for a period of 12 consecutive months. The Agencies request comment on whether the examples are adequate and on whether the proposed standard deeming an account relationship to have terminated after 12 months of no communication is appropriate.

March 15, 2000

The final Rule should retain the examples, including the standard contained in the Proposed Rule deeming certain account relationships to have terminated after 12 months of no communication from an institution to a customer. As the Agencies correctly point out, certain customer relationships (such as obtaining investment advice from a financial institution) do not present a clear event after which there is no longer a customer relationship. The 12-month standard provided in the Proposed Rule sets forth a bright-line test that financial institutions can apply in determining when these types of account relationships have terminated. Without this bright-line test, financial institutions would face substantial uncertainty regarding whether many types of account relationships have terminated.

In addition, the Agencies request comment on whether, in the example of dormant accounts, the applicable standard should be state law, rather than the institution's policies. The final Rule should retain the institution's policies as the applicable standard with respect to the example regarding dormant accounts. This approach is consistent with the current standard established in Regulation E, which states that a financial institution need not provide periodic statements to consumers whose accounts become inactive as defined by the institution. Moreover, under state escheat laws, financial institutions often are required to wait from 5 to 10 years after activity on a deposit account has ceased before closing the account and turning over to the state any money in the account. Requiring a financial institution to continue to provide annual privacy notices to a customer on a deposit account for 5 to 10 years after activity on the account has ceased is excessive and would place sizeable unnecessary costs on financial institutions, without any corresponding benefits to customers.

March 15, 2000

**SECTION \_\_\_\_.6. INFORMATION TO BE INCLUDED IN SECTION 503 PRIVACY NOTICE.**

In General.

The Proposed Rule sets 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 Rule 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 Rule, 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. Also, because consumers are likely to receive Section 503 privacy notices from a broad range of financial institutions (typically 20 or more of such notices per consumer), the consumer will be overwhelmed if he or she receives lengthy, detailed notices from every "financial institution" with which the consumer has some type of relationship. A consumer is not likely to read any of the many Section 503 privacy notices he or she receives, because of the sheer length of each such notice.

In addition, by requiring overly detailed Section 503 privacy notices, the Proposed Rule would impose substantial additional burdens on financial institutions, with absolutely no corresponding benefit to consumers. In particular, the extraordinary level of detail required by the Proposed Rule would essentially preclude affiliated financial institutions from providing consumers with a combined Section 503 privacy notice for those institutions. Instead, given the level of detail contemplated, the Proposed Rule could even preclude a single financial institution from using one privacy notice for all of the institution's customers; since, as a practical matter, the Proposed Rule could essentially require a financial institution to provide different privacy notices for each of its product lines.

Moreover, by requiring overly detailed Section 503 privacy notices, the Proposed Rule would greatly increase the frequency with which financial institutions must provide change-in-terms notices regarding its privacy policy to consumers. For example, a financial institution could be forced to provide a change-in-terms notice to consumers each time the institution offers a new financial product or service, obtains information from a new source or establishes a marketing program with a new partner. These frequent change-in-terms notices from a myriad of financial institutions would create significant confusion on the part of consumers and would impose enormous costs on financial institutions. Furthermore, because of the substantial costs of providing these

March 15, 2000

change-in-terms notices, the Proposed Rule, as currently drafted, could stifle innovation with respect to financial products and services. For example, the Proposed Rule could effectively restrict the ability of a financial institution to change marketing arrangements, even if such changes would benefit the institution and its customers, because of the additional costs of providing change-in-terms notices.

Thus, unless the Agencies revise the examples, as discussed below, to reduce significantly the level of detail required for the Section 503 privacy notices, the final Rule will have the unintended consequence of harming consumers and financial institutions alike.

#### Categories of Information Collected.

The example in Section \_\_\_\_.6(d)(1) provides that a financial institution adequately discloses the categories of nonpublic personal information that the institution collects if the institution categorizes such information according to the source of the information, such as application information, transaction information and credit reports. This example should be revised to provide that a financial institution is only required to give *examples* of the categories of information that the institution collects. Requiring a financial institution to identify every possible category of information that the institution collects unnecessarily increases the length and complexity of the Section 503 privacy notice, resulting only in confusion on the part of consumers.

In addition, the example in Section \_\_\_\_.6(d)(1) should be revised to make it clear that a financial institution may categorize information collected by type of source, by content, or by a combination of both. As revised, this example would provide financial institutions with the flexibility they need in deciding how best to categorize nonpublic personal information that the institution collects. Also, it is critical that the example in Section \_\_\_\_.6(d)(1) be revised to refer to examples of the “type of source” rather than “source,” in order to make clear that a financial institution is not required to disclose the names of entities from which the nonpublic personal information has been collected, or even to identify every conceivable type of source from which information may be received.

#### Categories of Information Disclosed to Nonaffiliated Third Parties.

The example in Section \_\_\_\_.6(d)(2) provides that a financial institution adequately categorizes nonpublic personal information that the institution discloses when the institution categorizes such information according to source and provides illustrative examples of the content of the information. This example should be revised to make it clear that a financial institution is required to provide only *examples* of the categories of nonpublic personal information that the institution discloses. Requiring a financial institution to list each and every category of nonpublic personal information that may be disclosed would unnecessarily increase the length and complexity of the Section 503 privacy notice, without any accompanying benefit to consumers.

March 15, 2000

In addition, the final Rule should provide that a financial institution may categorize information disclosed by type of source, by content, or by a combination of both. The final Rule also should provide financial institutions with the flexibility they need to choose how best to categorize the nonpublic personal information that the institution discloses. In some cases, a financial institution simply may not know the source of the nonpublic personal information that it discloses. For example, with respect to accounts that a financial institution purchases from another entity, the institution would not have the information necessary to determine the types of sources from which the nonpublic personal information connected with these accounts was collected. Thus, the final Rule should provide financial institutions with the flexibility to categorize information disclosed solely by content.

#### Information Sharing Practices with Affiliates.

The Proposed Rule requires a financial institution's Section 503 privacy notice to include a detailed discussion of the institution's information sharing practices with respect to the institution's affiliates. In particular, under the Proposed Rule, a financial institution would be required to provide in its Section 503 privacy notice information about: the categories of nonpublic personal information that may be disclosed to affiliated third parties; the categories of affiliated third parties to whom such information may be disclosed; and the opt-out notice required, if any, under Section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act ("FCRA opt-out notice"). The inclusion of these affiliate-sharing provisions in the Proposed Rule is entirely inconsistent with the GLB Act. Section 503 of the GLB Act provides that except for the FCRA opt-out notice, a financial institution is not otherwise required to include in its privacy notice information relating to the institution's information sharing practices with affiliates.

More specifically, Section 503(a) of the GLB Act requires a financial institution to provide a privacy policy notice to customers, and Section 503(b) delineates the information to be included in the privacy policy notice mandated under Section 503(a). In particular, Section 503(b)(1) provides that a financial institution's privacy policy must include information regarding the policies and practices of the institution with respect to disclosing nonpublic personal information to "nonaffiliated third parties," including, among other things, the categories of persons to whom the information is or may be disclosed. Moreover, Section 503(b)(1) does not require that a financial institution include in its privacy policy information regarding the categories of nonpublic personal information that might be shared with affiliated third parties or the categories of affiliated third parties to whom such information might be shared. The only requirement related to affiliate sharing listed in Section 503(b) is the reference to the FCRA opt-out notice.

This more focused reading of Section 503(b) also is consistent with the intended scope of Title V of the GLB Act, since Section 506(c) makes it clear that Congress intended Title V of the GLB Act to address only a financial institution's sharing practices with nonaffiliated third parties. Thus, to be consistent with the GLB Act, the final Rule should be revised to provide that except for the FCRA opt-out notice, a financial institution is not otherwise required to provide information in its Section 503 privacy

March 15, 2000

notice regarding the institution's information sharing practices with affiliated third parties.

#### Categories of Nonaffiliated Third Parties to Whom Information is Disclosed.

The example in Section \_\_.6(d)(3) provides that a financial institution adequately categorizes the nonaffiliated third parties to whom the institution discloses nonpublic personal information if the institution identifies the types of businesses in which the nonaffiliated third parties engage. The example further explains that a financial institution may use general terms to describe the types of businesses in which such third parties engage -- such as the term "financial products and services" -- but only if the institution also includes appropriate examples of the significant lines of businesses of the nonaffiliated third parties, such as consumer banking, mortgage lending, life insurance or securities brokerage. This example should be revised to specify that a financial institution may categorize nonaffiliated third parties to whom information is disclosed by type of business in which such entities engage, by type of products offered by those entities, or by a combination of both. The final Rule should make it clear that financial institutions have the flexibility to choose how best to categorize the nonaffiliated third parties to whom they share nonpublic personal information.

#### Section 502(e) Exceptions.

The Proposed Rule indicates that with respect to the exceptions in Section 502(e), a financial institution is required only to inform consumers that it makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the institution's Section 503 privacy notice. The Agencies request comment on whether this notice is adequate. This notice of the Section 502(e) exceptions is more than adequate to inform a consumer that a financial institution may be disclosing nonpublic personal information relating to the consumer to nonaffiliated third parties, other than those described in the Section 503 privacy notice, as permitted by law. A more lengthy, detailed discussion of the Section 503(e) exceptions would unnecessarily increase the length and complexity of the Section 503 privacy notice, potentially confusing consumers without providing them with meaningful information or additional benefits. It would also increase the circumstances where financial institutions would be required to provide costly change-in-terms notices with no possible corresponding consumer benefits.

#### Right to Opt Out.

Under Section \_\_.6(a)(6) of the Proposed Rule, a financial institution would be required to provide in its Section 503 privacy notice information about the consumer's right to opt out under Section 502, including the methods by which the consumer may exercise that right. The final Rule should not require the inclusion in the Section 503 privacy notice of a duplicative explanation of the consumer's right to opt out under Section 502; the explanation of this opt-out right should be reserved for the Section 502 notice. Requiring the Section 503 privacy notice to contain an additional explanation of the Section 502 opt-out right would unnecessarily increase the length and complexity of

March 15, 2000

the Section 503 privacy notice, potentially confusing consumers without providing them with meaningful additional information.

If the final Rule continues to discuss the Section 502 opt-out right in connection with the Section 503 privacy notice, the Agencies should make it clear in the final Rule that they are not suggesting that this is an additional Section 503 privacy notice requirement, but only that when the Section 502 opt-out notice is provided, it should be accompanied by the Section 503 privacy notice.

#### Confidentiality, Security and Integrity of Information.

The example in Section \_\_\_\_6(d)(5) indicates that a financial institution adequately describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if the institution explains who has access to the information and the circumstances under which the information may be accessed. The example further provides that a financial institution adequately describes its policies and practices with respect to protecting the integrity of nonpublic personal information if the institution explains the measures it takes to protect that information against reasonably anticipated threats or hazards.

This example regarding confidentiality and security should be revised to provide that a financial institution need only provide examples of the types of limitations, if any, that the institution places on access to information. Requiring a financial institution to provide detailed information in its Section 503 privacy notice regarding who has access to nonpublic personal information of consumers and the circumstances relating to such access would unnecessarily add to the length and complexity of the Section 503 privacy notice, without providing meaningful information to consumers.

In addition, the example regarding integrity should be deleted entirely in the final Rule. While Section 503 of the GLB Act refers to the “confidentiality and security” of nonpublic personal information, it includes no reference to the term “integrity.” To the extent that the Agencies consider a financial institution’s practices in protecting the “integrity” of nonpublic personal information to be *different* from the institution’s practices in protecting the “security” of such information, the reference to “integrity” should be deleted because the statute does not require financial institutions to disclose their practice in protecting the “integrity” of information. On the other hand, to the extent that the Agencies consider the concepts of “integrity” of information and “security” of information to be the *same*, the reference to “integrity” still should be deleted as duplicative because the Proposed Rule already contains an example regarding “security” of information. In either case, the final Rule should make no reference to integrity of information because any such reference would either be duplicative or beyond the scope of the statute and, thus, inappropriate in an already too detailed notice.

#### **SECTION \_\_\_\_7. SECTION 502 OPT-OUT NOTICE.**

March 15, 2000

### Joint Accounts.

The Agencies request comment on how the right to opt out should apply in the case of joint accounts. In particular, the Agencies ask whether a financial institution should require all parties to an account to opt out before the opt out becomes effective. A financial institution should be required to provide the Section 502 opt-out notice to only one party to the account. This approach is entirely consistent with other consumer protection regulations, such as Regulation Z and Regulation E, which generally provide that disclosures required under those consumer protection regulations need be provided only once in connection with the opening of any account. As is the case with these existing regulations, the party who receives the Section 502 opt-out notice also would receive it as a representative on behalf of other parties to the account.

Similarly, where a financial institution provides the Section 502 opt-out notice to one party to the account, the financial institution should be prepared to honor an opt out from any party to the account. Thus, with respect to joint accounts, an opt out received from any party to the account should be honored with respect to all nonpublic personal information relating to that account. Nonetheless, the final Rule should provide flexibility to financial institutions with respect to how opt-out notices are provided to, and received from, the parties to a joint account. For example, a financial institution should be allowed to provide a single notice for a joint account and if any party to the joint account opts out, the institution would honor that opt out with respect to the nonpublic personal information of all parties to the joint account. Alternatively, the final Rule should permit, but not require, a financial institution, if it is willing and has the operational capability to do so, to provide a separate opt-out opportunity for each party to the account, so that one account customer could permit the financial institution to share that customer's nonpublic personal information with third parties, while permitting the other account customer to opt out of such sharing. Providing financial institutions with this flexibility with respect to joint accounts is consistent with the partial opt-out provision already contained in the Proposed Rule, which allows a financial institution the option of providing consumers with the opportunity to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

### Reasonable Opportunity to Opt Out.

The Proposed Rule provides that a consumer must be given a reasonable opportunity to opt out before information is disclosed. Specifically, the Proposed Rule provides two examples of when a financial institution has complied with the reasonable standard -- one example for opt-out notices for "consumers" who engage in isolated transactions with the institution and one example for notices that are provided to "customers" of the institution.

#### *Example for Isolated Transactions.*

March 15, 2000

The example pertaining to isolated transactions indicates that a financial institution has provided a reasonable opportunity to opt out to a consumer engaged in an isolated transaction with the institution if the institution provides the consumer with the Section 502 opt-out notice at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction. This example, as currently drafted, is entirely inconsistent with the GLB Act. In particular, Section 502 of the GLB Act does not require that the Section 502 opt-out notice be provided to a consumer at the time of the isolated transaction between the consumer and the financial institution. Instead, under Section 502, a financial institution is clearly allowed to provide the Section 502 opt-out notice to a consumer *at any time* before nonpublic personal information relating to that consumer is disclosed to a nonaffiliated third party, so long as the institution provides the consumer with a reasonable amount of time to opt out of such disclosures after that Section 502 opt-out notice is given.

In addition, the Proposed Rule, by requiring financial institutions to provide the Section 502 opt-out notice (as well as the Section 503 privacy notice) to consumers at the time of the isolated transaction, would impose enormous costs on financial institutions, without any benefits to consumers. For example, with respect to ATM transactions, such a requirement would force a financial institution to incur the tremendous costs of reconfiguring all of its ATMs to provide the Section 502 opt-out notice (as well as the Section 503 privacy notice) to every person who uses one of the institution's ATMs, either through a screen disclosure on the ATM or by use of a detailed notice posted at the ATM, and the institution would be required to modify such on-site disclosures any time its information practices change. Because of the enormous costs of doing so, financial institutions would be precluded, as a practical matter, from sharing nonpublic personal information relating to any consumers who engage in isolated transactions with the institution with nonaffiliated third parties. Thus, the Proposed Rule would turn the opt-out restriction in Section 502 into an outright prohibition on financial institutions sharing nonpublic personal information about consumers who engage in isolated transactions with the institution. In addition, requiring a financial institution to provide the Section 502 opt-out notice (as well as the Section 503 privacy notice) to a consumer at the time of the isolated transaction would also significantly inconvenience the consumer. For example, with respect to ATM transactions, a consumer will not want to scroll through the Section 502 opt-out notice (and the Section 503 privacy notice) before completing an ATM transaction.

For all of these reasons, and to be consistent with the statute, the example regarding isolated transactions should be revised to provide that a financial institution may provide the Section 502 opt-out notice to a consumer that is engaging in an isolated transaction with the institution either: (1) at the time of the transaction; or (2) at a later time, so long as no nonpublic personal information of the consumer is disclosed to a nonaffiliated third party before the Section 502 opt-out notice is provided and the customer is given a reasonable amount of time to opt out. In addition, the example should be revised to provide that if the opt-out opportunity is given at the time of the

March 15, 2000

transaction, a financial institution may provide the opt-out opportunity at any time during the transaction, including after the transaction has been completed.

*Mailed Notices to Customers.*

The example relating to mailed notices specifies that a financial institution provides a “consumer with whom it has a customer relationship” with a reasonable opportunity to opt out if the institution mails the Section 502 opt-out notice (and the Section 503 privacy notice) to the customer and allows the customer a reasonable period of time, such as 30 days, to opt out.

This example should be revised to apply to all consumers, not just customers. A financial institution should be allowed to use the mail as a method to provide the Section 502 opt-out notice to all consumers, including consumers who engage in isolated transactions with the institution. The example also should be revised to specify that if the Section 502 opt-out notice is provided through the mail to a consumer and an address is specified as a method for the consumer to opt out, the institution must allow the consumer a reasonable amount of time to exercise the right to opt out -- such as 30 days - - before information is shared. In addition, the Proposed Rule should be revised to make it clear that a financial institution can specify in its Section 502 opt-out notice a toll-free telephone number as a means to opt out, and that this is a reasonable opt-out method, if the institution allows the consumer a reasonable amount of time, such as 15 days, to exercise the right to opt out before any information relating to the consumer is shared with nonaffiliated third parties.

*Electronic Medium to Opt Out.*

The Agencies seek comment on whether an example in the context of transactions conducted using an electronic medium would be helpful. The final Rule should include an example which specifies that a financial institution may provide the Section 502 opt-out notice (and the Section 503 privacy notice) to a consumer by using electronic mail if the consumer has agreed to receive information by electronic delivery. In addition, the final Rule should make it clear that if a financial institution provides the Section 502 opt-out notice to such a consumer by using electronic mail, the consumer has a reasonable amount of time -- such as 15 days -- to exercise the opt-out right before information may be shared.

**SECTION \_\_\_\_.8. FORM AND METHOD OF PROVIDING SECTION 502 OPT-OUT NOTICE.**

March 15, 2000

Examples of Reasonable Means to Opt Out.

The example in Section \_\_\_\_8(a)(2)(ii) of the Proposed Rule specifies 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 Rule, however, specifies 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.

This example should be revised to make it clear that the use of toll-free telephone numbers provides a reasonable means to opt out. In this regard, the FTC in its proposed privacy regulations, provides that a financial institution may designate a toll-free telephone number as a means that consumers can use to opt out. Both consumers and financial institutions would benefit by allowing a financial institution to provide a toll-free telephone number as a means that consumers can use to opt out. Consumers can simply make a toll-free call to opt out. In addition, financial institutions would be provided the flexibility they need in providing opt-out methods that meet their needs, as well as the needs of their customers.

Moreover, in drafts of the Proposed Rule originally released by the Agencies, the Agencies had provided that the reply form should be in the form of a detachable, pre-addressed form or self-addressed, stamped reply card. In addition, the FTC's proposed privacy regulations, as officially released, contain an example relating to reply forms which contemplates that a self-addressed stamped envelope would be included with the detachable reply form. The FTC's example relating to detachable forms with self-addressed, stamped envelopes is excessive and would impose enormous costs on financial institutions, without benefiting consumers. In fact, requiring a financial institution to provide any type of reply form, even if a self-addressed, stamped envelope is not required, to each and every consumer to whom the institution mails a Section 502 opt-out notice would be extremely costly to financial institutions, especially smaller institutions.

Thus, the example referencing a reply card should be replaced with one indicating that providing an address for opt out, together with clear instructions on how to do so, is sufficient. Specifying an address where a consumers can write to opt out provides consumers with a meaningful means to exercise their opt-out rights, without imposing enormous costs on financial institutions in providing reply forms. Nonetheless, if the Agencies do retain the example pertaining to reply forms in the final Rule, it is absolutely imperative that the Agencies include the example relating to toll-free telephone numbers, as discussed above. Without the ability to provide toll-free telephone numbers as a means to opt out, financial institutions, especially smaller institutions, would face unnecessary and unjustified costs in providing the Section 502 opt-out opportunity to consumers.

March 15, 2000

In the Supplemental Information included with the FTC's proposed privacy regulations, the FTC requests comment on whether financial institutions should be required to accept opt outs through any means the institution has already established to communicate with consumers. For example, if a financial institution has established a toll-free telephone number for its customer service department, should the institution be required to accept opt outs at that number? The final Rule should make it clear that a financial institution is not required to accept opt outs through any means the institution has already established to communicate with consumers, but instead can designate a specific contact point for this purpose. Requiring a financial institution to accept opt outs through any means would force the institution to incur the enormous costs of establishing and implementing procedures to train all employees who interact with consumers in any way to handle opt-out requests, and would make it far more likely that consumer opt-out requests will not be given effect. Such a requirement could force financial institutions to curtail the methods or avenues through which consumers may communicate with the institution, to the detriment of consumers and institutions alike.

#### Oral Contracts.

The Proposed Rule provides that if a financial institution and a consumer orally agree to enter into a customer relationship, the institution may provide the Section 502 opt-out notice within a reasonable time thereafter, if the consumer agrees.

Requiring a financial institution to provide the Section 502 opt-out notice within a reasonable time after the oral agreement is wholly inconsistent with Section 502 of the GLB Act. Under Section 502, a financial institution is allowed to provide the Section 502 opt-out notice to a consumer *at any time* before nonpublic personal information about that consumer is shared with nonaffiliated third parties, provided the consumer is given a reasonable amount of time to opt out after the notice is given before information is shared with nonaffiliated third parties, and the final Rule should be modified accordingly.

#### Continuing Right to Opt Out.

The Proposed Rule explains that a consumer may exercise the right to opt out at any time, and a financial institution must comply with the consumer's direction as soon as reasonably practicable after receiving the customer's request. In the Supplemental Information included with its proposed privacy regulations, the FTC requests comment on whether the final Rule should specify a specific time period within which a financial institution must implement these opt outs. The final Rule should not specify a specific time period, and should retain the "reasonably practicable" standard set forth in the Proposed Rule. Because the operational structure and practices of financial institutions vary widely, the setting of one time period with which all financial institutions must abide is inappropriate and would be extremely difficult to implement. The "reasonably practicable" standard adequately protects the privacy interests of consumers without placing undue operational and cost burdens on financial institutions.

March 15, 2000

Duration of Consumer's Opt-Out Direction.

The Proposed Rule provides that a consumer's direction to opt out under Section 502 of the GLB Act is effective until revoked by the consumer in writing, or if the consumer has agreed to accept notices in electronic form, in electronic form. The final Rule should allow a consumer to revoke an opt-out direction orally. Specifically, the final Rule should not deny consumers convenient ways to reverse their opt-out decision, such as enabling them to do so orally either by telephone or in person.

**SECTION \_\_\_9 EXCEPTIONS RELATING TO SERVICE PROVIDERS AND JOINT MARKETING AGREEMENTS**

Agents, Processors and Service Providers.

Section \_\_\_9, as currently drafted, would have a disastrous effect on financial institutions, especially smaller institutions. In crafting the disclosure and opt-out provisions of Title V of the GLB Act, Congress intended to add wide-ranging consumer privacy protections without interfering with longstanding, essential outsourcing practices of banks and other financial institutions. Thus, Congress exempted various common servicing activities in two separate places: in Section 502(b)(2) and in Section 502(e). The combination of these two provisions was intended to allow a financial institution to continue to outsource to agents, processors, or other service providers *any* activities that the financial institution could perform itself.

Section 502(b)(2) of the GLB Act provides that the notice and opt-out requirements of the Act do not apply where information is provided to third parties who perform services for, or functions on behalf of, the financial institution. Section 502(b)(2) also exempts certain joint financial institution marketing programs, provided that they meet specified statutory requirements. In drafting the proposed implementing regulations, however, the Agencies have inappropriately applied the disclosure and confidentiality requirements of Section 502(b)(2), intended for joint financial institution marketing arrangements, to traditional bank outsourcing arrangements, unless those arrangements also qualify under Section 502(e).

The failure to correct this inappropriate treatment of outsourcing arrangements would create substantial costs for financial institutions, especially smaller institutions, with absolutely no corresponding benefits to consumers. This rule would mean, for example, that a financial institution could not hire a mailing firm to send information to its own customers, other than monthly statements, without complying with these special disclosure and confidentiality rules. Also, an institution could not retain an outside company to develop scoring models, evaluate applications or do reference checks (all common practices, particularly for small banks) without satisfying these same special rules.

March 15, 2000

More specifically, under Section \_\_\_\_9 of the Proposed Rule, a financial institution would be required to include in its privacy policy disclosures, for most of its existing outsourcing arrangements, a separate description of the categories of information that are disclosed and the categories of third parties providing the outsourced services. In complying with these requirements, the financial institution must provide the same level of detail that is required to satisfy the requirements for disclosing information to all other third parties. In addition, under Section \_\_\_\_8 as proposed, a financial institution cannot change its outsourcing arrangements -- at least as to the types of information disclosed or the types of third-party service providers utilized -- unless and until it sends a change-in-terms notice to *all* of its customers. In other words, in order to economically justify the use of a new service provider, the financial institution would not only have to consider the cost savings of using this new service provider, but then also weigh these cost savings against the costs of sending change-in-terms notices to *all* of its customers.

Such a misguided rule would be very costly for large banks who are members of bank holding companies, but at least they may have the option of using an affiliate for some of their outsourcing needs. But, for smaller institutions, such a requirement would be a disaster, since any cost savings that might be gained by a possible outsourcing arrangement would be eliminated by the costs of preparing, printing and mailing new privacy notices to all of the institution's customers. And for what purpose? Absolutely none, since no opt-out rights exist for such outsourcing arrangements, and none can be justified so long as the information transferred can only be used for the servicing purposes contemplated. In addition, there is no apparent policy reason why outsourcing activities under Section 502(b)(2) should be treated any differently than outsourcing activities under 502(e). In both cases, a financial institution is making information available to its own agents, processors and servicers to perform activities that the institution would otherwise do itself, because the third party can perform the activity cheaper or better, or both. In neither case should this be viewed as the "sharing" of information with a nonaffiliated third party; instead, the servicer should be viewed simply for what it is -- an extension of the financial institution, performing services that the financial institution would otherwise perform itself.

The special disclosure and confidentiality requirements should be restricted to their intended application -- information shared between two or more financial institutions in connection with a joint marketing arrangement involving those nonaffiliated financial institutions. If the Agencies believe, however, that some outsourcing disclosure is necessary, it should be brief and generic: "We may use third party processors and servicers to assist us, and share with them information to allow them to do so." To require otherwise would turn every outsourcing decision into an economic burden on financial institutions and consumers alike, with no accompanying benefits.

Contractual Agreement.

March 15, 2000

Under Section \_\_\_\_.9, the contractual agreement in connection with joint marketing arrangements must specify that the third party will use the information solely for the purposes for which the information is disclosed or as otherwise permitted by Section 502(e). With respect to this contractual agreement requirement, the Agencies request comment on whether third-party contractors should be permitted to use information received pursuant to Section \_\_\_\_.9 to improve credit scoring models or analyze marketing trends, so long as the third party does not maintain the information in any way that would permit identification of a particular consumer; that is, to use depersonalized or aggregate information for modeling purposes.

The final Rule should permit third-party contractors to depersonalize information received pursuant to Section \_\_\_\_.9 and use such information for other purposes -- such as improving credit scoring models or analyzing marketing trends. First, the use by third-party contractors of such aggregate information for the purpose of improving credit scoring models falls within the “necessary to effect, administer or enforce a transaction” exception under Section 502(e)(1). Specifically, the disclosure of such aggregate information for credit scoring models is “usual . . . to carry out . . . the product or service business to which the transaction is a part . . .” because the development and utilization of scoring systems is not only common, but has become an essential element of the credit approval process. In addition, because the information would be depersonalized, the privacy interests of consumers are not lessened in any way by allowing third parties to use information received under Section \_\_\_\_.9 for such purposes.

#### Joint Marketing Agreements.

In the Joint Notice, the Agencies seek comment on whether the Proposed Rule should be revised to require a financial institution to take steps to assure itself that the product being jointly marketed and the other participants in the joint marketing agreement do not present undue risks for the institution. The Agencies indicate that these steps could include ensuring that the financial institution’s sponsorship of the product or service in question is evident from the marketing of that product or service.

The Agencies should not impose additional requirements on financial institutions with regard to joint marketing arrangements. Due to the Agencies’ tight deadline for issuing the final Rule, the Agencies simply do not have the time before the final Rule must be issued to consider adequately whether additional requirements are necessary to protect the interests of consumers and financial institutions. In addition, the Agencies should not hastily impose additional requirements on joint marketing arrangements, but should first wait and see whether the statutory requirements of full disclosure and confidentiality agreements are adequate to protect the interests of consumers and financial institutions. In this regard, the Agencies can always revisit the issue of whether additional requirements beyond the statutory requirements are needed with respect to joint marketing programs.

The Agencies also seek comment on whether the Proposed Rule should provide examples of the types of joint agreements that are covered. The Agencies should not

March 15, 2000

attempt to add examples of the types of joint agreements to the final Rule. Again, the Agencies can always add such examples at a later time, if they feel further clarification is needed regarding what types of arrangements qualify as joint agreements.

## **SECTION \_\_\_\_ .10. EXCEPTIONS RELATING TO TRANSACTION PROCESSING.**

Sections \_\_\_\_ .10(a)(2) and (a)(3), respectively, provide that the Section 502's obligations in providing the privacy notice and the opt-out notice to a consumer do not apply when an institution is disclosing the consumer's nonpublic personal information: (1) "to service or process a financial product or service requested or authorized by the consumer;" or (2) "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." To be consistent with Section 502(e) of the GLB Act, the phrase "in connection with" should be added to the beginning of the clauses in Sections \_\_\_\_ .10(a)(2) and (a)(3).

In particular, Sections 502(e)(1)(A) and (B) of the GLB Act provide that the Section 502's obligations in providing privacy notices and opt-out notices to consumers do not apply if the institution is disclosing nonpublic personal information "in connection with" servicing or processing a financial product or service requested or authorized by the consumer; they similarly do not apply "in connection with" maintaining or servicing 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. This "in connection with" language is essential because it makes it clear that the exceptions in Sections 502(e)(1)(A) and (B) (as implemented by Sections \_\_\_\_ .10(a)(2) and (a)(3) respectively) include activities that relate to servicing or processing a financial product or service or maintaining or servicing the consumer's account, even where these activities are not absolutely necessary to service or process the financial product or financial service or to maintain or service the consumer's account.

## **SECTION \_\_\_\_ .11. OTHER EXCEPTIONS.**

### With Consent or Direction of the Consumer.

#### *Co-brand and Affinity Program.*

In certain credit or debit card arrangements, it is contemplated that the consumer has or will have a relationship with both a financial institution and a nonaffiliated third party which also is participating in the program (a so-called "co-brand" or "affinity" program). For example, a financial institution may offer a co-branded credit card with an airline company, where cardholders would receive benefits (such as frequent flier miles) from the airline company based on use of the credit card. As is the case with all such

March 15, 2000

rewards programs, the benefits program provided by the airline company is offered in conjunction with the credit card program, essentially as one product. These types of co-brand or affinity programs benefit consumers and financial institutions alike.

The final Rule should make it clear that co-brand and affinity programs are matters of notice and consent, rather than notice and opt out. In such co-brand or affinity programs, the relationship agreement itself contemplates that the consumer has or will have a relationship with both the financial institution and the co-brand or affinity partner, and the benefits program is offered by the co-brand or affinity partner in conjunction with the debit or credit card program, essentially as one product. The sharing of information by the financial institution with the co-brand or affinity partner is an integral part of offering that product. As a result, the sharing of information by a financial institution with a co-brand or affinity partner should be a matter of notice and consent, rather than notice and opt out. The consumer has chosen to participate in this arrangement which necessarily involves use of the information by both the financial institution and the co-brand or affinity partner in connection with what is essentially the same customer relationship.

Also, the final Rule should specify that if a consumer participating in a co-brand or affinity program later opts out of sharing, a financial institution 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. The addition of the following example would accomplish both of these goals: “When a customer enters into a credit or deposit arrangement with [you/the bank] in which it is contemplated in the relationship agreement that the consumer will have a relationship with both [you/the bank] and a nonaffiliated third party that also is participating in the program (such as a “co-brand” or “affinity” program), the consumer has consented to [your/the bank’s] sharing of the customer’s nonpublic personal information with that third party in connection with the co-brand or affinity program by entering into that relationship arrangement. If the consumer participating in the co-brand or affinity program later opts out of sharing under §\_\_\_8(d), [you/the bank] may terminate the account or shift the consumer to another account.”

#### *Consent Safeguards.*

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.

The final Rule should provide financial institutions with flexibility with respect to the methods by which financial institutions may obtain consent from a consumer. Specifically, the final Rule should not require that a consumer’s consent be in writing or indicated on a separate line in a relevant document or on a distinct Web page. Instead,

March 15, 2000

the final Rule should only require that the consent provision be presented in a clear and conspicuous manner to the consumer.

Requiring a consumer's consent to be in writing would actually harm consumers as well as financial institutions. In some instances, it may be impossible or impractical for a financial institution to obtain a consumer's consent in writing in a timely fashion. For example, the example in Section \_\_\_\_ .11(b) of the Proposed Rule provides that a consumer may specifically consent to a financial institution's disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to the institution for a mortgage so that the insurance company can offer homeowner's insurance to the consumer. However, if oral consent were not accepted, a consumer who applies for a mortgage over the telephone simply would not have the opportunity to obtain the homeowner's insurance quote in a timely manner, to the detriment of the consumer.

With respect to standards relating to the scope of consent, the Agencies, at most, should only require that the consent provision be specific in its terms, such that the consent provision identifies the particular purposes for which information will be disclosed and the types of information that will be disclosed. In particular, the consent provision should not be required to identify nonaffiliated third parties to whom the information will be disclosed, other than by type of business, because the identity of the third party may differ based on the circumstances and the consumer's geographical location.

This approach to the scope of the consent provision is consistent with the approach used under the Fair Credit Reporting Act ("FCRA"). For example, in its credit applications, a financial institution often may obtain the consent of a consumer to provide the loan application file to another lender for that lender's consideration of the application, if the institution decides not to extend the credit. This type of referral program benefits both consumers and institutions alike. Under a so-called "joint user exception" to the FCRA, a financial institution would not become a consumer reporting agency under the FCRA as a result of sharing a consumer's loan application file with another lender for use by that lender in considering the application, so long as the institution has the consumer's consent to such sharing.<sup>4</sup> In an informal FTC staff letter on the "joint user exception," the FTC staff indicated that the consent provision need not indicate the particular name of the third party to whom the loan application file may be forwarded; instead the FTC staff indicated that a provision which enables the consumer to indicate consent for the loan application file to be forwarded to "other lenders" is sufficient for FCRA purposes.<sup>5</sup> Similarly, the final Rule should not require the financial institution in the consent provision to identify nonaffiliated third parties to whom the information will be disclosed, other than by type of business.

On the other hand, to the extent that the consent provision is able to identify the particular nonaffiliated third party to whom information will be disclosed, the final Rule

---

<sup>4</sup> See 16 C.F.R. pt. 600, App., comment 8 to § 603(f).

<sup>5</sup> FTC Interpretive Letter from Helen G. Foster to Linda J. Throne, November 20, 1998.

March 15, 2000

should allow the financial institution to describe more broadly the particular purposes for which information will be disclosed with that nonaffiliated third party. This is particularly important in co-brand and affinity programs, where, as described above, the relationship agreement itself often contemplates that the consumer has or will have a relationship with both the financial institution and the co-brand or affinity partner. Specifically, with respect to consent provisions in connection with co-brand or affinity relationships, the financial institution should not be required to specify in detail the particular purposes for which information will be disclosed or the types of information that will be disclosed to the co-brand or affinity partners, if the institution identifies the co-brand or affinity card partner and states that the shared information will be used in connection with the co-brand or affinity relationship.

## **SECTION \_\_\_\_.12. LIMITS ON REDISCLOSURE AND REUSE OF INFORMATION.**

### Redisclosure of Information by a Third Party.

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. A financial institution should not be required to affirmatively 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 whom 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.

### Reuse of Information by a Third Party.

The Proposed Rule provides that a nonaffiliated third party may use nonpublic personal information about a consumer that it receives from a financial institution in accordance with an exception under Sections \_\_\_\_.9, \_\_\_\_.10 or \_\_\_\_.11 only for the purpose of that exception. The final Rule should allow the nonaffiliated third party to reuse the information if the so-called “secondary use” falls within one of the exceptions in Sections \_\_\_\_.10 or \_\_\_\_.11. Because the “secondary use” falls within one of the exceptions in Sections \_\_\_\_.10 or \_\_\_\_.11, the nonaffiliated third party could simply re-obtain the information from the financial institution for the “secondary use” purpose. The final Rule should not require the nonaffiliated third party to undergo this additional step of obtaining the information from the financial institution. Instead, the final Rule should allow a nonaffiliated third party to reuse information for a secondary purpose if this secondary purposes falls within one of the exceptions in Sections \_\_\_\_.10 or \_\_\_\_.11.

March 15, 2000

**SECTION \_\_\_\_ .13. LIMITS ON SHARING OF ACCOUNT NUMBERS FOR MARKETING PURPOSES.**

Agents, Processors and Service Providers.

The Proposed Rule should make it clear that the providing of account numbers by a financial institution to its agent, processor or service provider that is supplying 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 GLB Act. Congress did not intend the Section 502(d) prohibition to restrict the ability of a financial institution to provide account numbers to the institution's agents, processors and other service providers that perform services on the institution's behalf or otherwise assist the institution in servicing its own customers and prospective customers. Instead, Congress intended Section 502(d) to restrict the ability of a financial institution to provide account numbers for a credit card account, deposit account or other transaction account of a consumer to a nonaffiliated third party for use by *that* nonaffiliated third party in marketing *that* third party's good or services. Congress simply did not intend to interfere with longstanding outsourcing practices of banks and other financial institutions.

However, without a clarification in the final Rule that the providing of account numbers by a financial institution to the institution's agents, processors or service providers is not prohibited by Section 502(d), financial institutions may be required to discontinue certain routine practices of using agents, processors and service providers because of the uncertainty surrounding whether such practices are prohibited under Section 502(d). For example, financial institutions often disclose account numbers to a service provider who handles the preparation and distribution of monthly checking account and credit account statements for the institution. In many cases, the institution also directs the service provider to include marketing literature with the statement about a product; in some cases, the account number may be preprinted on the response form to ensure proper account posting. Section 502(d) simply does not apply to this type of practice. First, a financial institution -- in making information available to its processors and service providers engaged in activities on the institution's own behalf -- should not be viewed as "sharing" information with a nonaffiliated third party. Instead, the processor or service provider should be viewed as an extension of the financial institution itself. In addition, for this particular practice, a financial institution would be providing the account numbers to service providers for its own statement and marketing purposes.

Nonetheless, without clarification that such practice is not covered by Section 502(d), a financial institution may be required to discontinue this practice because of uncertainty regarding whether the practice is prohibited by Section 502(d). The final Rule should make it clear that the providing of account numbers by a financial institution to its own agent, processor or service provider 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 GLB Act.

March 15, 2000

Encrypted Account Numbers and Reference Numbers.

The final Rule should make it clear that the term “account number or similar form of access number or access code” does not include an account number or other similar number, so long as that number is encrypted when provided to the nonaffiliated third-party marketer and the nonaffiliated third-party marketer is not given the information or device needed to decode or unscramble the encrypted number. In addition, the final Rule should clarify that the term “account number or similar form of access number or access code” does not include a so-called 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 by the recipient nonaffiliated third-party marketer to post a charge or debit against the particular account.

As the Agencies discuss in the Joint Notice, the Section 502(d) prohibition is designed to avoid the risks associated with direct access by a third party to a consumer’s account, whereby the third party can directly post charges or debits to the consumer’s account by using the account number. These risks are not present, however, when encrypted account numbers or so-called reference numbers are used, where the third-party marketer cannot use these numbers to post a charge or debit against a consumer’s account. In addition, when a consumer agrees to purchase goods or services from a nonaffiliated third party and agrees to use a credit card or debit card account for this purchase, the third party needs some accurate device to identify for the financial institution which account should be debited or charged. Encrypted account numbers and reference numbers serve this important purpose of allowing a third party to identify accurately to the institution which account should be debited or charged, without imposing risks regarding unauthorized use of the consumer’s account.

Transaction Account.

The final Rule should make it clear that the term “transaction account” as used in Section 502(d) does not apply to a mortgage or other installment loan where no charges can be posted to the loan balance by the third-party marketer. The risks associated with third parties’ direct access to a consumer’s account --such as unauthorized debits or charges to the account -- simply are not present in those cases where a third-party marketer cannot post charges to the loan balance of the mortgage or other installment loan.

Consent.

The final Rule should 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 to provide that information to that nonaffiliated third-party marketer.

March 15, 2000

This consent provision is particularly important in the context of co-brand or affinity credit or debit card programs. A financial institution often makes available account numbers relating to the co-brand or affinity accounts to the co-brand or affinity partners, so that when the co-brand or affinity partner communicates information relating to the accounts to the financial institution, the co-brand or affinity partner can accurately identify the account to which the information relates. As discussed above, the sharing of information by a financial institution with a co-brand or affinity partner -- including account numbers -- should be a matter of notice and consent. The consumer has chosen to participate in this arrangement which necessarily involves use of the information by both the financial institution and the co-brand or affinity partner.

#### Conclusion of Marketing Activities.

The final Rule 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.

This clarification is consistent with the plain language of Section 502(d), which only restricts a financial institution from providing an account number for a credit card account, deposit account or transaction account of a consumer to any nonaffiliated third party "for use in" telemarketing, direct mail marketing or other marketing through electronic mail to the consumer. Once a consumer has decided to purchase the good or service being marketed, the marketing has concluded. Nonetheless, to avoid confusion regarding when the marketing activities have concluded, the final Rule should clarify 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.

#### **SECTION \_\_\_\_ .16. EFFECTIVE DATE; TRANSITION RULE.**

The Agencies seek comment on whether six months following the adoption of the final Rule is sufficient time to enable financial institutions to comply with the regulations. In actuality, a financial institution would not even have six months to comply with the obligations of Sections 502 and 503 with respect to existing consumers to whom it is disclosing information. In the Joint Notice, the Agencies indicate that if a financial institution intends to disclose nonpublic information about someone who was a consumer before the effective date of the regulations, the institution must provide the Section 502 opt-out notice (and the Section 503 privacy notice) to the consumer and provide a reasonable opportunity to opt out before the effective date.

The final Rule should provide that while the obligations of Sections 502 and 503 of the GLB Act and the implementing regulations become effective six months following the adoption of the Final Rule, compliance with such obligations is voluntary until 12

March 15, 2000

months after the effective date (*i.e.*, until November 13, 2001). Sections 502 and 503 of the GLB Act place numerous new obligations on financial institutions. Indeed, financial institutions will not know the true extent of the obligations imposed under Sections 502 and 503 until the final Rule is released; thereafter, financial institutions need adequate time to implement operational changes and audit procedures which are necessary to comply with these obligations. In addition to developing Sections 502 and 503 notices, financial institutions must establish and implement new procedures for delivering such notices to consumers. Moreover, financial institutions must establish and implement new procedures for providing opt-out methods to consumers and for receiving and handling opt outs received from consumers. Financial institutions also must design and implement effective employee training programs for satisfying all of these new procedural requirements, and must establish compliance systems to adequately monitor the institutions' performance in complying with these requirements. Furthermore, financial institutions also must evaluate all of their existing contracts with nonaffiliated third parties, to determine if they comply with the obligations imposed under Sections 502 and 503. Most of these activities require significant computer system changes that financial institutions need time to implement.

Requiring financial institutions to complete hastily all of these enormous system changes within six months of when the final Rule is released would almost ensure mistakes on the part of financial institutions, to the detriment of institutions and consumers alike. Thus, the final Rule should provide that the obligations of Sections 502 and 503 of the GLB Act and the implementing regulations become effective six months following the adoption of the final Rule, but compliance with such obligations is voluntary until 12 months after the effective date.

Although this voluntary compliance rule should apply to both new and existing customers of the institution, it is absolutely critical that the final Rule adopt a voluntary compliance rule of 12 months with respect to existing customers of financial institutions. For existing customers, the Proposed Rule provides that a financial institution is required to provide the Section 503 privacy notices within 30 days of the effective date of regulations. This 30-day transition period is simply too short a time frame for financial institutions to provide the Section 503 privacy notice to existing customers. With this 30-day transition period, financial institutions would be required to provide a Section 503 privacy notice to each and every one of their existing customers by December 13, 2000. Thus, financial institutions would be required to provide these Section 503 privacy notices during the holiday season -- one of the busiest times for mail during the year. In addition, financial institutions are already overburdened this time of year preparing to send other special year-end disclosures to consumers -- such as notices for tax purposes. In addition, the privacy notices undoubtedly will generate a great number of calls to financial institutions regarding the privacy rights of their customers and the meaning of the elements of a very complex privacy notice. These calls are likely to overwhelm the customer call centers of financial institutions, since the holiday season already is one of the peak times for customer service calls.

March 15, 2000

The short 30-day transition period also would place tremendous pressure on financial institutions in finding third-party service organizations to prepare and print their privacy notices and to provide these notices to consumers on behalf of the institutions. In many cases, financial institutions use third-party mail houses to process and send notices to consumers on behalf of the institution. If each and every financial institution is required to send a Section 503 privacy notice to all of their existing customers within the same 30 days, these mail houses -- which are limited in number -- will be completely overwhelmed. In fact, because of this market demand, financial institutions may be required to pay exorbitant fees to these mail houses in order to retain their services in mailing out the notices. Moreover, the 30-day transition period will not allow an institution to coordinate the mailing of Section 503 privacy notices with other required disclosures that are mailed out-- such as periodic statements -- because the 30-day period might not necessarily overlap with the time period in which the next periodic statement must be mailed out.

For all of these reasons, it is imperative that the final Rule provide financial institutions sufficient time within which to send out the Section 503 privacy notices to existing customers. A voluntary compliance rule of 12 months would provide financial institutions with the flexibility they need in providing the Sections 502 and 503 notices to all of their existing customers.

In the final Rule, the Agencies also should make it clear that if an institution attempts to establish and implement reasonable procedures to comply with the obligations of Sections 502 and 503 of the GLB Act, as implemented by the final Rule, the institution's failure to comply with such obligations should not be considered a violation of the statute if the violation results from an inadvertent error. This concept of a safe harbor from inadvertent errors is essential if financial institutions are not given adequate time after the final Rule is released to comply with the obligations under Sections 502 and 503.

\* \* \* \*

We appreciate the opportunity to comment on this important subject. If we can assist you further, or if you have any questions regarding the above, please feel free to call at 650/432-3111.

Sincerely yours,

Russell W. Schrader