



**Nancy Baran**  
Assistant General Counsel

**The Prudential Insurance Company of America**  
751 Broad Street, Newark NJ 07102-3777  
Tel 973 802-8133 Fax 973 643-5520

March 31, 2000



Jennifer J. Johnson  
Secretary  
Board of Governors of the  
Federal Reserve System  
20<sup>th</sup> 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 17<sup>th</sup> 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 5<sup>th</sup> 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 Mesdames:

The Prudential Insurance Company of America (“Prudential”) appreciates the opportunity to provide its comments on the proposed privacy rules implementing Title V of the Gramm-Leach-Bliley Act (“GLB Act” or “Act”). Prudential is a mutual insurance company with affiliates engaged in a wide variety of financial activities. It is a diversified unitary savings and loan holding company, and its affiliates include a federal savings bank, a state chartered bank, and four broker-dealers. Prudential is also the manager of a family of registered investment companies and provides investment advisory and administrative services for them. Thus, like many other financial institutions, Prudential and its affiliates will be affected by the privacy regulations adopted by several federal regulatory agencies. In addition, Prudential and its insurance affiliates are subject to regulation by several state insurance regulators for GLB Act Title V purposes.

We are submitting these comments to each of the seven federal regulators which have published proposed regulations because the seven regulations address very similar issues, and we believe that consistent regulations for all entities that must comply with GLB are necessary.

Prudential applauds the federal regulators for producing proposed regulations for the respective regulated industries that are consistent and comparable. We respectfully suggest that it is important that the final regulations be workable for diversified financial services organizations as well, including the new financial holding companies which the Act authorizes. To the extent that the final regulations are used as models by state insurance regulators in publishing their own GLB Act implementing regulations, it would be very helpful if the final federal regulations were sufficiently flexible to address these issues where that is practical. We have therefore included comments on these points below.

Long before GLB Prudential had made privacy an important part of its business. Based on its experience, Prudential has serious reservations about the notices that the proposed rule would require. These points are discussed in detail in the more specific comments below, and we point them out here more generally.

- The proposed rule, particularly some of the examples, require that far too much detail be included in the notices, and compliant notices will not be useful to consumers or customers.
- They will create serious operational constraints for financial institutions that cannot change some of their outsourcing activities without mailing new notices.
- The rule requires notices to be clear and conspicuous, but the volume of detail mandated will cause the notices to be lengthy and complex, as opposed to clear.
- Affiliated companies will have to provide different privacy notices, even when their privacy policies are identical, because the complexity and volume of detail called for by the proposed rule and the examples will render impossible a single, common notice that is accurate for all affiliates.

Comment has been requested regarding the inclusion of examples in the rule. The examples are very helpful for ascertaining the application of the rule, and Prudential

appreciates the effort that has been devoted to developing realistic examples for the respective regulated businesses. Our comments below suggest some additional examples that may also be helpful. The rule should indicate that the examples are merely illustrative and are not intended to foreclose compliance in any manner permitted by the rule.

Prudential's more specific comments on the proposed regulations are provided below in the order of the sections of the proposed regulations to which they relate. Where comments are provided in response to one or more agencies' request for specific comments, they are included with the section to which they most closely relate.

### **Section \_\_\_\_ .3, Definitions**

*Clear and conspicuous: Clarify and simplify the "clear and conspicuous" requirements.*

The definition of "clear and conspicuous" includes examples which create complex compliance requirements for financial institutions in providing compliant notices. Notices which satisfy the standard may still not be clear and conspicuous, and clear, conspicuous notices can be developed without satisfying all nine of the criteria that the first two examples require. Prudential respectfully submits that the rule should be modified to allow substantially more flexibility for financial institutions to provide "clear and conspicuous" notices.

*Consumer: Clarify that individuals are not consumers when financial institutions do not routinely receive information about them.*

Two of the examples in the Securities and Exchange Commission's proposed rule address a point that is, in a broader sense, common to many financial institutions. Prudential respectfully recommends that the regulators all address it in a modification to the definition of "consumer" proposed in the text below. The last two examples in the SEC's proposed rule address issues relating to securities held or issued by a financial institution which does not have information about the identity of the individual having a beneficial interest in the securities. Similar issues arise for depository institutions which may not have nonpublic personal information about individuals whose accounts are held in the names of custodians, guardians, or other legal representatives; or for whose benefit funds are held by third party escrow agents. Insurance companies have the related issue of group insurance contracts with employers under which insurance coverage is provided to the employer's employees, but about which employees the insurer does not receive any identifying information. In these cases, employers remit premium without identifying the covered employees.

In each of the instances described above, the financial institution does not have nonpublic personal information about an individual who has some type of interest in the financial product. The GLB Act does not by its terms require that privacy notices be provided to

such individuals, and the proposed rule does not either. It would be a useful clarification of the proposed rule, to add a sentence that parallels the language in the SEC example which says that an individual is not a consumer when the financial institution does not routinely receive information about the individual.

*Government regulator: Expand the definition to encompass all state as well as federal financial institution regulators.*

The proposed rule defines “government regulator” to mean the eight regulators listed in GLB section 505(a) plus the Secretary of the Treasury. This term is used in subsections \_\_\_\_\_.11(a)(4) and \_\_\_\_\_.11(a)(7)(iii) of the proposed rule, and refers to regulators to which disclosures of nonpublic personal information may be made without notice or opt out. Financial institutions are subject to the jurisdiction of regulatory authorities in addition to those listed in GLB section 505(a), for example, state securities regulators, state banking authorities, and state insurance regulators in each state where insurers are licensed, and they may be required to release information to those regulators. The definition of “government regulator” should be expanded to include all those regulators.

*Personally identifiable financial information: Modify the definition to exclude information that is not financial.*

The proposed rule treats all personally identifiable information of a consumer as “personally identifiable financial information,” even when the information is not financial in nature. As the first example for each alternative definition in the proposed rules points out, even medical information would be included. This definition goes well beyond both the GLB language and Congress’ intention, which was to address financial information in particular. Congress expressly removed references to medical information in the financial services modernization bills in order to treat that subject separately. The proposed rule should be modified to address financial information without sweeping in other types of non-financial information such as medical or demographic information, and examples to clarify the narrowed definition should be included in the revised rule.

*Comment regarding application of definition to data not containing personal identifiers.*

Comment has been requested regarding whether “nonpublic personal information” covers information that does not contain any indicators of a consumer’s identity, with the example given of aggregated mortgage loan data containing no personal identifiers being provided to a third party to prepare market studies. This type of information is not “personally identifiable,” since no natural person could be identified from the data described. If not “personally identifiable,” information is not “nonpublic personal information” as defined by the Act.

Additionally, there would seem to be no privacy-related public purpose that is served by restrictions on sharing this kind of information. Since no person could possibly be identified, no personal privacy issue is raised. Moreover, this information is really information about the institution itself in that it describes attributes of its assets, liabilities, customer base, or market, rather than “nonpublic personal information” about a consumer or which could be linked to a consumer. We respectfully submit that information that does not contain any indicators of a consumer’s identity is not “nonpublic personal information,” and recommend that the definition be revised accordingly. Additional examples would be useful to assist in the application of a narrowed rule as well.

#### **Sections \_\_\_\_\_.4 and \_\_\_\_\_.5, Initial and Annual Notices to Consumers**

*Timing of Initial Notice: The rule should follow the Act and permit initial notices to be given at or before the time the customer relationship is established.*

The proposed rule requires initial notices to be provided to consumers prior to establishing a customer relationship. This timing is not supported by the statutory language that refers to providing the notice at the time a customer relationship is established. The proposed rule reduces or eliminates the financial institution’s ability to provide a privacy notice at the same time as it delivers other important customer disclosures and notices, and may even require a separate mailing for this single document. Consumers would receive important information about financial products and services in piecemeal fashion. Sensible, prudent business practice would provide all relevant documents to consumers at the same time, both to facilitate consumers’ actual review of the documents and the transaction, and to permit efficient operations for the institution. Modification of the proposed rule to require notices to be provided at or before establishing a customer relationship would enhance consumer convenience and business processing, as well as conform to the standards of GLB section 503.

*Electronic Notices: Modify the rule to allow institutions to provide a current rather than the actual historical version of electronically delivered privacy notices.*

The proposed regulation requires that initial notices which are provided electronically be maintained by the financial institution so that customers may obtain them in writing at a later time. Institutions would be required to maintain electronic notices indefinitely. The public policy of providing customers with information regarding the handling of their information would be fully satisfied by a regulation that required that customers who received electronic notices be provided with a copy of the privacy notice that is current at the time of the customer's request for a written copy. The current notice is the relevant document for customers in any event, so it would be the better document to provide. Prudential suggests that the final rule be modified accordingly.

*Common, Single Notices: Clarify rule to allow common, single notices where they are accurate.*

The commentary in the Supplementary Information sections of the Joint Notice and the Federal Trade Commission's notice says, "The proposed Rule does not prohibit affiliated institutions from using a common initial annual or opt out notice, so long as the notice is delivered in accordance with the Rule and is accurate for all recipients." The Securities and Exchange Commission's Supplementary Information section takes a similar position. This point is well taken, and we believe it should be incorporated into the final rule. We point out that the simpler privacy notices recommended in our comments regarding \_\_\_\_\_.6 above would be required to effectuate common, single privacy notices for affiliates, since the volume of detail required by the proposed rule would render notices inaccurate for an institution's affiliates.

Prudential respectfully suggests that the final rule expand the application of this concept and expressly permit affiliated institutions to provide common annual privacy notices to their customers, i.e., a single annual privacy notice, when the conditions in the commentary quoted above are satisfied. A customer having multiple relationships with affiliated institutions would thus still receive annual privacy notice that applies to all of the relationships, and diversified financial services organizations could realize more of the efficiencies which affiliations have the potential to engender. In addition, when a financial product or service is issued or provided by one affiliate, and sold by another affiliate, the final rule should make it clear that only a single privacy notice need be provided so long as the affiliates' privacy policies are the same. We suggest that the final rule include another example to clarify this point.

*Providing Notice; Oral Agreements: Modify the rule to require delivery of privacy notices within a reasonable time after an oral agreement to establish a customer relationship and to remove the requirement for a formal “agreement” to receive the notice later.*

In subsection (d) *How to provide notice*, the proposed rule permits delivery of the initial privacy notice to consumers within a reasonable time after the customer relationship is established when the financial institution and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice later. The consumer’s agreement to receive the notice later is implicit in the decision to establish the relationship, and the requirement for a formal “agreement” to receive the notice later would produce a very awkward conversation. Prudential recommends that the rule be revised to require that the notice be provided within a reasonable time after the conversation.

*Notices to Multiple Account Holders: Clarify that a single initial or annual privacy notice is required for multiple parties on a single account.*

In instances where more than one individual is party to a single financial institution service or product, a single initial and annual privacy notice should be sent to the name and address provided by the parties for other communications respecting the account. Generally only a single address is provided for a single copy of account information to be provided to the account holders, and very often a financial institution has only one address for the parties on an account in any event. Even given the importance of privacy protection, no public policy purpose is served by requiring more copies of privacy notices than copies of other account documents to be sent to account holders.

*Clarify that when financial institutions have not communicated with a consumer for twelve consecutive months there is no continuing relationship.*

Section \_\_\_\_\_.5(c)(2) of the proposed rules contains examples of “termination of customer relationship” occurring when communications with the account holder about the account have ceased, even though the account holder’s account remains open on the financial institution’s books. Insurance companies face the same issues other financial institutions face in this regard. Given the commonality of this issue, Prudential suggests that the language contained in the depository institutions’ proposed rules at \_\_\_\_\_.5(c)(2)(iv) and the FTC proposed rule at \_\_\_\_\_.5(c)(2)(iii), all of which are identical, be moved from the examples into the text of the final rule adopted by all the regulators at \_\_\_\_\_.5(c)(1). The SEC’s example at \_\_\_\_\_.5(c)(2)(iv) should remain as an example.

**Section \_\_\_\_ .6 Information to be included in initial and annual notices**

*Categories of Information: Modify the examples to simplify notices, and delete the requirements for reporting sources and examples.*

The GLB Act Section 503 requires that privacy notices disclose the categories of information collected by the institution, and the categories of information that may be disclosed by the institution. The proposed rule defines “categories” in the examples to require identification by source for the former, and identification by source accompanied by illustrative examples for the latter. The detail required by these definitions will result in privacy notices that are very long and cumbersome, and the specificity required will foreclose any possibility that diversified financial institutions may use a single, common notice in those instances where the diversified institution has a single policy for all customers. Consumers having multiple relationships with financial institutions and their affiliates will receive multiple, different, notices that appear conflicting, even though the identical policy may govern each of their relationships with these companies.

Financial institutions will be compelled to label each piece of data they maintain to identify its source in order to comply with the proposed rule. Substantial modifications to their information systems would be required to allow this. Customers can be fairly apprised about the categories of information collected and disclosed without this complex labeling.

“Clear and conspicuous” disclosure is simpler than the disclosure that the proposed rule’s examples require. Full and fair disclosure of the information collecting and disclosure practices of financial institutions can easily be achieved by notices that are far less detailed than the examples.

The GLB Act demolished the barriers to financial institution affiliations, and created financial holding companies to encourage affiliations. This provision of the proposed rule creates a new barrier, and it even sows distrust of the institutions in consumers’ minds because of the different, apparently conflicting, notices it requires. Prudential respectfully suggests that the rule be modified by eliminating the current examples referring to “source” and “illustrative example” of information. Replacement examples should be added that do not include requirements for these details, and are substantially simpler and more flexible.

*Descriptions Required for Section \_\_\_\_ .9 Disclosures: Modify the rule to say that disclosures to nonaffiliated third parties may be made as permitted by law.*

Subsection \_\_\_\_ .6(a)(5), as applied to disclosures of customer information to service providers, suffers from the overburdening with detail described above. The application of this standard to unaffiliated third parties that provide services other than joint marketing has the potential to cripple financial institution operations, and it is not required by the GLB Act.

When Congress enacted GLB, it understood that financial institutions rely on a variety of third party service providers in the normal course of business, and it intended sections 502(b)(2) and 502(e) to permit this outsourcing to continue uninterrupted. Section 502(b)(2) requires financial institutions to “fully disclose” that they provide nonpublic personal information to unaffiliated third parties for service purposes, but it does not prescribe detailed listings of information.

Financial institutions use unaffiliated third parties for many kinds of activities relating to the marketing of their own products and services, including the very cross-selling the GLB Act was enacted to encourage. Frequently the third party must have customer information to perform its obligation. Financial institutions use such vendors because they have expertise or resources the institution lacks, or they may be able to provide the service less expensively than the institution can. The amount of detail required by the proposed rule would require financial institutions to provide revised customer privacy notices to all customers before they could modify their servicing arrangements if the new servicing had not been adequately described by category of information and category of service provider in the previous notice. The expense of providing these notices, perhaps even in a separate mailing, would inhibit change and growth and would weld financial institutions to the status quo.

This result defies Congress’ objective of modernizing financial services with the passage of the GLB Act. GLB does not provide an opt out from financial institutions’ use of nonpublic personal information to obtain services from third parties. Consequently, we cannot conceive of any consumer benefit that could reasonably result from consumers receiving the revised notices required by this subsection that would “balance” the related cost. Prudential strongly urges that the proposed rule be modified to provide that a financial institution has fully disclosed its arrangements with service providers if it advises customers that it makes disclosures to other nonaffiliated third parties only as permitted by law.

*Disclosure of Policies and Practices to Protect Information: Modify the rule to require description of financial institutions’ policies to protect confidentiality and security.*

The GLB Act and the proposed rule require disclosure of the financial institution’s policies to protect the confidentiality and security of nonpublic personal information. The proposed rule goes well beyond the Act and requires, in addition, disclosure of financial institutions’ practices respecting protecting the confidentiality and security of this data, and their policies and practices respecting protecting the integrity of the data.

The example in the proposed rule provides that an institution has adequately described its policies and practices for protecting security and confidentiality if it explains who has access to the information and the circumstances under which access may be had. Describing who has access to nonpublic personal information and the circumstances under which access is provided would result in quite a lengthy tome for most financial institutions. Financial institution personnel in many different disciplines whose work is

required to effect, administer and enforce customer transactions of all kinds all have access to various subsets of nonpublic personal information under a multitude of circumstances. In addition, numerous third parties have appropriate, necessary access to nonpublic personal information under still different sets of circumstances, many of which are exempted from the notice requirements by GLB Section 502(e).

Description of policies and practices respecting protecting data integrity are adequate under the proposed rule when the institution explains the measures it takes to protect against reasonably anticipated threats or hazards. The required description would mandate descriptions of data backup, data storage, disaster recovery and numerous other institutional safeguards in place to protect one of the institution's most valuable assets. None of this is included in the Act.

The proposed rule requires such a large volume of detailed information that frequent revisions will likely be required to keep the notice current. Those revised notices would need to be provided to customers more frequently than annually to apprise customers of changes in the handling of nonpublic personal information. The cost of such mailings would be substantial, and the likely result would be that financial institutions would adopt new approaches and adapt to new challenges less rapidly than they otherwise might. This is an extraordinary price to pay for a form whose details are not required by the law and are not beneficial to consumers. Prudential respectfully submits that all parties, financial institutions and their customers alike, would be best served by a modification of the rule and the illustrative examples to return to the GLB Act disclosure requirements of describing the policies the institution maintains to protect the security and confidentiality of data.

*Description of Nonaffiliated Third Parties Subject to Exceptions: Modify the rule to eliminate this provision.*

Comment has been requested regarding the adequacy of the description contained in Section \_\_\_\_\_.6(b) regarding disclosures to exempted third parties. Section 502(b)(1)(A) of the GLB Act excepts disclosures made to these nonaffiliated third parties from any notice or opt out. Thus, the Section \_\_\_\_\_.6(b) requirement is not supported by the Act. For this reason, the description certainly should not be expanded. We believe that the description should be retained in the rule, but only for the purpose described above relating to descriptions required for \_\_\_\_\_.9 disclosures, and any reference to disclosures authorized by sections \_\_\_\_\_.10 and \_\_\_\_\_.11 should be removed.

## **Section \_\_\_\_ .12 Limits on Redisclosure and Reuse of Information**

*Financial institutions should not be required to develop policies and procedures to ensure third party compliance.*

Comment has been requested regarding whether the rule should require financial institutions which disclose information to unaffiliated third parties to develop policies and procedures to ensure that the third party complies with the disclosure limits. Customer data is one of the most important assets of financial institutions, and it is generally protected by contractual provisions addressing its treatment and handling when it is disclosed to unaffiliated third parties. Should a breach occur, the financial institution has the ability to address it as any other breach of contract problem would be addressed. No public policy or business reason requires a different standard for handling privacy issues, and the cost of “ensuring” the compliance of unaffiliated third parties would be very high, for no discernible benefit. In addition, the Act makes recipients of financial institutions’ nonpublic personal information subject to its requirements and enforcement by the appropriate regulator.

## **Section \_\_\_\_ .16 Effective Date; Transition Rule**

*Interim Final Rule: The regulators should adopt an interim final rule in lieu of a final rule.*

Prudential believes that the regulators have done outstanding work in developing a proposed rule that applies to many diverse financial institutions and businesses, in an area of tremendous complexity. The GLB Act and the proposed rule raise difficult issues, which we expect will be the subject of many comments. We respectfully suggest that the agencies adopt an interim final rule based on these comments, and continue to accept further comments with the possibility for modifications to the interim rule based on the further comments. This would permit the continuing of productive communications among the regulators, financial institutions, and other interested parties before the rule is adopted in its final form.

*Effective Date: The effective date for the rule should be amended to November, 2001.*

The proposed rule includes an effective date of November 13, 2000. Having developed, implemented, and mailed notices regarding its customer privacy policy for a substantial portion of its business, Prudential respectfully suggests that this timing will be impossible for financial institutions to meet. Assembling the information for inclusion in the notices will be difficult for financial institutions, and compliance will require that it be accurate and verified, adding to the time needed. For many financial institutions, formulating their information sharing policies will also be difficult and time consuming. If our experience is any guide, the privacy notices that the rule requires will require very substantial

systems development work on many systems and databases, much of which must be done seriatim rather than in parallel. Training and communications for large, disparate groups of employees must be developed and accomplished. Customer materials will need to be developed and printed. Prudential's experience was that developing its policy, systems, training, communications, and customer materials consumed a little more than one year, with the mailing to existing customers being spread over a second year to allow the notices to be included in regular mailings, to avoid the high costs of a separate mailing. We respectfully suggest that the effective date be one year later than the date in the proposed rule to permit financial institutions to implement an orderly process and develop sound policies and procedures to implement the GLB privacy notices.

*Transition rule: The transition rule should be modified in accordance with the proposed modification of the effective date and also to avoid separate mailings.*

The proposed transition rule gives thirty days after the rule's effective date for providing initial notices to existing customers. This would require separate mailings for those customers, which would be exorbitantly expensive for financial institutions. In addition, for the reasons discussed above regarding the effective date, financial institutions will be unable to meet the timing required by the proposed rule. Prudential suggests that the regulators modify this subsection in a manner consistent with the proposal regarding the effective date above.

Prudential appreciates the opportunity to comment on this matter of central importance to financial institutions of all kinds. If you have any questions about these comments, please call me at 973 802 8133.

Very truly yours,

