

COMMENTS OF
CONSUMERS UNION
CONSUMER FEDERATION OF AMERICA
US PUBLIC INTEREST RESEARCH GROUP
ON JOINT AGENCIES' PROPOSED RULES
ON
PRIVACY OF CONSUMER FINANCIAL INFORMATION

March 31, 2000

Office of the Comptroller of the Currency
Docket No. 00-05

Board of Governors of the Federal Reserve System
Docket No. R-1059

Federal Deposit Insurance Corporation
Comments/OES

Office of Thrift Supervision
Docket No. 2000-13

Federal Trade Commission
Gramm-Leach-Bliley Act Privacy Rule, 16 CFR Part 313 Comment

COMMENTS OF
CONSUMERS UNION
CONSUMER FEDERATION OF AMERICA
US PUBLIC INTEREST RESEARCH GROUP
ON JOINT AGENCIES' PROPOSED RULES
ON
PRIVACY OF CONSUMER FINANCIAL INFORMATION

INTRODUCTION

These comments respond to a Joint Notice of Proposed Rulemaking, 65 Fed. Reg. 8770 (February 22, 2000), on Privacy of Consumer Financial Information. Consumers Union¹, the Consumer Federation of America² (CFA), and the US Public Interest Research Group (PIRG)³, appreciate this opportunity to comment⁴ on draft regulations to implement Title V of the Gramm-Leach-Bliley Act. Consumers Union, CFA, and US PIRG, ("the Consumer Groups") together with other advocacy organizations, played an active role in seeking strong and meaningful financial privacy protections for American consumers during the congressional debate on the Gramm-Leach-Bliley Act (the "GLB" or "financial modernization act.")

Because there are only minor differences in each agencies' draft, these comments are comprehensive and will be filed with each agency in response to the joint notice, as well as to the Federal Trade Commission in response to their proposed rule.

The Consumer Groups are skeptical that financial privacy will be protected by the proposed rule because of the flaws in the underlying legislation. The GLB falls far short of providing meaningful

¹ Consumers Union, publisher of *Consumer Reports* magazine, is an independent, nonprofit testing and information-gathering organization, serving only the consumer. We are a comprehensive source of unbiased advice about products and services, personal finance, health, nutrition, and other consumer concerns. Since 1936, our mission has been to test products, inform the public, and protect consumers.

² Consumer Federation of America is a nonprofit association of more than 260 pro-consumer organizations with a combined membership of more than 50 million people. CFA was founded in 1968 to advance the consumer interest through advocacy and education.

³ U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups. PIRGs are non-profit, non-partisan consumer and environmental advocacy groups with members around the country.

⁴ In the future, should several agencies submit joint notices, consumers should be given the opportunity to file only one set of comments that would be considered by each of the agencies. The Consumer Groups note that because of the notice published jointly there might be confusion about the filing of comments. Given the heightened public interest in the privacy issue, we encourage that the agencies review comments jointly and that each agency gives consideration to all comments even if those comments were filed with only one agency in response to the joint notice. The Consumer Groups encourage other agencies to adopt the format for filing comments used by the FDIC for those consumers choosing to file comments electronically.

privacy protections. Therefore these regulations are inherently flawed, despite the best efforts of the regulators to craft a suitable rule.

Loopholes in the law and in this draft rule allow personal financial information to be shared among affiliated companies without the consumer's consent. In many instances, personal information can also be shared between financial institutions and unaffiliated third parties, including marketers, without the consumers consent. Other loopholes allow institutions to avoid having to disclose all of their information sharing practices to consumers. In addition, neither the GLB nor these draft regulations allow consumers to access to the information about them that an institution collects. **While the agencies cannot close loopholes in the law, the draft regulations should be strengthened to ensure that they do not add any new loopholes.**

Promulgation of these regulations does not mean the end of the debate over financial privacy. Senators Shelby and Bryan and Representatives Markey and Barton, along with others in Congress, have already introduced legislation to plug the loopholes in the modernization bill and provide meaningful privacy protections for consumers. Because the GLB left to the states the issue of adding stronger protection, many states are moving to enact stronger privacy laws.

We will continue to work with the agencies and other interested parties to promote the passage of meaningful privacy protections and rules.

General Comments on the Proposed Rule: Financial Privacy Not Yet a Reality

With the passage of the GLB, the financial marketplace is poised to undergo rapid and profound changes, including the consolidation of industries. One consequence is that personal financial information has become a marketable commodity, with banks, insurance companies and securities firms knowing, and having the capacity to know, more about an individual consumer than ever before. Not only is this information used to market products and services to consumers, it can be used to make decisions about the cost and availability of those products and services.

Consumers have reason to be concerned about how their private financial information is being collected, used, shared and sold. Under the GLB there are no limits on the ability of a financial institution to share information about consumers' transactions, including account balances, who they write checks to, where they use a credit card and what they purchase, within a financial conglomerate. Because of loopholes in GLB, in most cases sharing a consumer's sensitive information with a third party is allowed too. All the exceptions created by GLB, and therefore included in the proposed rule, make it difficult to come up with a list of circumstances where personal financial information cannot be shared. Unfortunately, regulators' are prevented from going beyond the failings of the GLB in drafting these regulations. Nonetheless, we believe that the regulations could be improved and we provide specific suggestions on how the regulations should be tightened.

Here is why the GLB and the proposed regulations fail to provide privacy protections:

- **Limited notice provisions.** The notice provisions merely require that an institution provide consumers with the institution's privacy policy, which could simply say "We share your information with affiliates and third parties." Financial institutions would only have to provide general information about the type of information that is collected and with whom it is shared. A consumer would not have to be told how their information is being used. In some cases the proposed regulations do not require that an institution provide a consumer with any notice at all, such as when the information collected is used to service an account.
- **Opt-out to "nonaffiliated third parties" only.** GLB's limited third party opt-out does not apply at all to internal affiliate sharing -- affiliates can still share and sell information. Consumers will have no ability to stop it.
- **Loopholes gut the already limited opt-out requirement by allowing information to be shared with "nonaffiliated third parties" under most circumstances.** Even if a consumer wants to opt-out, information may still be shared with third parties offering financial products on behalf of or endorsed by the institution or pursuant to a joint agreement between financial institutions. Thus, financial institutions can share customers' information without notice to the customer or permission from the customer.
- **No consumer access.** The law does not allow a consumer to have access to the information collected, or the ability to correct erroneous information.

Here is what consumers should have when it comes to privacy protections:

- **Notice:** Financial institutions should inform their customers in a clear and conspicuous manner when they plan to collect, use and/or disclose personally identifiable information, and customers should be told the intended recipient of the information and the purpose for which it will be used. Notice should be about the sharing of information with all entities, both internal and external, and for any reason, including the servicing of accounts.
- **Access:** A customer should have access to all personally identifiable information held by the financial institution to make sure it is accurate, and complete and customers should the ability to correct erroneous information. These rights should not only be limited to account information, but should extend to any dossiers, profiles or other compilations prepared for sale or sharing with third parties.
- **Consent:** A financial institution should receive prior affirmative consent of the customer before it uses and/or discloses that customer's information for any other purpose than for which it was originally given. No customer should be denied, or forced to pay a higher price for, any product or services by a financial institution for refusing to give consent to the disclosure of the customer's personal information except where necessary to determine eligibility for a specific financial product or service.

Specific Comments on the Proposed Rule:

Section .1 Purpose and scope.

It is appropriate that the scope of information and institutions covered by the rule be broad. The ability to collect and use information about consumers is mind-boggling. Once collected, personal data may be used for many reasons, including profiling, marketing and decision-making. Recent actions by financial institutions and comments by a regulator reveal the intent of these institutions - to become data warehouses for both financial and non-financial information collected from and about individual consumers⁵. Any information collected by an institution from any source about an individual is available to be used as part of the process of determining how much a consumer may be charged for a product or whether a consumer should be marketed to or his or profile or account information should be shared or sold.

We support allowing the Federal Trade Commission (FTC) to promulgate regulations that will apply to institutions engaged in financial activities that are not traditionally considered to be financial in nature. Such broad application of the privacy provision was clearly the intent of Congress when it passed the GLB. This approach recognizes the wide range of financial activities in which a wide variety of businesses are currently engaged.

For example, many of the entities subject to the FTC's jurisdiction are involved in offering subprime financial products and services (such as debt collectors, money transmitters, check cashers, and payday lenders). The customers of these businesses often have less leverage to protect themselves than do mainstream banking customers. These vulnerable consumers need effective privacy protection to guard against exploitation and discrimination. For example, it has been widely reported that lenders, especially, but not limited to, sub-prime lenders, have failed to report full trade line information to credit bureaus. This practice results in consumers becoming captive customers of their own institution and its affiliates, and prevents the marketplace from working.

The broad approach proposed in these regulations also recognizes the reality of the marketplace and how information is shared. One of the most serious violations of financial privacy to date occurred not with a "third party" outside of the financial institution, but with a corporate subsidiary. In 1998, NationsBank (now Bank of America) paid a \$6.8 million in civil penalties to federal and state regulators when NationsSecurities used customer information obtained from NationsBank to sell risk adverse consumers uninsured derivative products. The consumers had low-risk certificates of deposit that were about to roll over, and were targeted for the sale of the risky derivative instruments. Thousands of conservative investors lost portions of their life savings.

Many financial institutions that are covered under the proposed rule offer what are often considered non-financial products. Information obtained from or about a customer may be

⁵ Speech by Julie Williams, Chief Counsel to the Comptroller of the Currency, before the Cyberbanking and Electronic Commerce Conference, Washington, DC, February 24, 2000.

commingled or so closely interrelated that it is impossible to keep the information separate. It is consistent with the intent of GLB that all the information obtained by a covered institution be subject to the proposed rule, whether that information is collected directly from a consumer, indirectly through transaction or experience data, or from a third party.

The rules should apply to any institution actively soliciting business in the U.S. Foreign financial institutions that solicit business in the U.S. should be subject to these rules. However, consumers should be afforded the stronger privacy protections where the country in which the business is located has more stringent privacy laws.

Section .2 Rule of Construction.

The use of examples is useful so long as the examples do not limit the regulators scope when looking at potential enforcement issues. It is difficult to contemplate all potential concerns or practices, as these may change over time.

Section .3 Definitions.

While the definitions and distinctions contemplated by the agencies may be useful in the overall scope of the privacy debate, they are fundamentally of little significance when considered within the flawed framework of GLB and the entirety of the proposed rule. Whether information is considered public or nonpublic, or an individual is considered to be a consumer or customer, or all information collected about an individual is considered to be personal financial information is moot if an institution is allowed to share that individual's data without his or her knowledge or consent.

The definitions and distinctions do not prevent information from being shared among affiliates, or under the exceptions contained in the proposed rule. In fact, focus on these definitions may confuse consumers and customers. Consumers and customers may be led to believe that because the information they provide to an institution is nonpublic and personally identifiable that they have to be provided notice about how the information is used and with whom it is shared. They may also be led to believe that they will be given the opportunity to consent to the sharing of their nonpublic and personally identifiable information when, in fact, that is not always the case.

Having noted our concerns above, we offer the following comments on the specific definitions contained in the proposed rule:

Q. (n) Nonpublic personal information.

The agencies are right to exercise caution on the distinction between public and nonpublic personal information. The ability to gather information about an individual consumer is astounding. Many consumers have no idea that information about them is collected, kept in a database, or available through the Internet. The consumer may reasonably expect that much of that information is private or nonpublic.

We support the agencies' conclusion that any list, description, or other grouping of consumers that is derived using "personally identifiable financial information" is nonpublic personal information.

Given the almost every day advances in technology, broad interpretations based on current perceptions of what is public or private may be of little use in defining these terms. Consumers should be accorded a reasonable expectation of privacy, and at least be alerted to the types of information where no privacy expectations should exist, because the information will be deemed (rightly or wrongly) to be public.

The definition of nonpublic personal information should be strengthened to include biometric information such as fingerprints, iris scans and the like. While not specifically discussed in the authorizing legislation, this information is much more personal than some other information that will qualify under the current definition of nonpublic personal information.

Q. (o) Personally identifiable financial information.

We agree with the principle that any information collected by an institution about an individual should be defined as personally identifiable. This includes information obtained directly from the individual, i.e., from an application, from transaction or experience data, or from other sources. In these instances, but for the financial nature of the relationship, the information would not be collected.

Q. (p) Publicly available information.

The agencies should not allow institutions to make assumptions about what could be obtained from "public" records. Information that may appear on its face to be "available" may not, in reality, be obtainable. For example, many Americans have an unlisted telephone number and address, so one cannot assume that everyone's name and number is publicly available because of a perception that such information appears in a phone book. If the information is not obtainable, it should not be considered available. The rules propose two alternatives for comment. Alternative A provides that an institution must actually obtain the information considered to be public, from a public source. Alternative B allows for an institution to make an assumption about whether or not personal information may be available from a public source without actually having to obtain that information from the public source. Alternative B could result in businesses attempting to pushing more information into the public sphere in order to avoid privacy obligations.

We strongly urge the adoption of alternative A for the definition of nonpublic personal information. While we find both proposed definitions to have too many exceptions, the added exception in alternative B of other publicly available information will be extremely difficult to enforce effectively. A financial institution might always argue that information that it did receive directly from a customer would have been publicly available if it had sought that information from some other source. Because of the proliferation of information about individuals available in commercial databases, it would be a dangerous precedent to permit financial institutions to escape

the restrictions of GLB for information provided by customers merely because the financial institution received the information from some other "publicly available" source.

The agencies have also requested comment on how to treat information obtainable from Internet sites, where those sites are available to the general public, and do not require a password or similar restriction. Simply because information is available online does not mean that it is "publicly available." Because the security of data cannot be guaranteed, it is possible to post nonpublic data on an unrestricted site. For example, credit card account access numbers were recently obtained by a hacker from a site and posted at another site that anyone could access. The agencies should make clear in the rule that information that is otherwise nonpublic should not be considered public merely because of its posting on the Internet.

In addition, the regulations request comment on how the Internet should be treated in the use of the term "widely distributed media." We believe that not every Internet site, particularly not those sites which are available only with payment of a fee, should qualify as widely distributed media from which information is publicly available. We therefore suggest that definition P(2)(ii) be modified to read "publicly available information from widely distributed media include the information from a telephone booth, a television or radio program, a newspaper of broad circulation, or an Internet site which is generally known to the public and available to the general public without requiring a password or fee, or membership and/or similar restriction."

The agency should consider a further restriction on the definition of that type of Internet site that would be considered to make information publicly available. These kinds of further restraints on the definition will be necessary in order to insure that the exception exempts only information that is widely available to the general public and not virtually all information about a person merely because it is already somewhere on the Internet.

We support the agencies' decision that notices must be provided "prior to" disclosing nonpublic information. The disclosures are of little value if they come after private information has already been shared. In this context, however, the material describing section four seems erroneous. That material suggests that a consumer opening a credit card account need not receive the privacy notice until he or she makes the first purchase, receives the first advance, or becomes obligated for a fee or charge other than the application fee. If the credit card company is collecting an application fee, the relevant time for the consumer to know whether or not that company will be interfering with the consumer's privacy is before payment of the application fee. Thus, we suggest that the time for the disclosure of information to be given is before or with the application to enter into a customer relationship. In the credit card case, this would be before or with the credit card application and certainly before the payment of any application fee.

There are other important definitions that merit comment:

"Clear and Conspicuous" -- Industry analysts admit that their disclosures will be difficult for consumers to understand. Congress was clear that the notice provision under the GLB is intended to enable consumers to make appropriate choices. Such choices are impossible if institutions

write unintelligible tomes crafted so that consumers have little hope of understanding how their information is being collected and shared.

The agencies should take the following approach. First, the rule must make clear that notices must be written in plain English (just as this rule was required to be drafted). Second, the rule should prescribe acceptable content and language in the notices in more specific detail.

The definition of "clear and conspicuous" needs to be modified so that the general requirement in (b)(2)(i) continues to apply even if the bank meets the standard and uses the kind of display set forth in (b)(2)(iii). The basic standard in (ii) is that the bank "designs its notice to call attention to the nature and significance of the information contained in the notice." This standard should be required whether or not the bank merely uses larger type sizes [perhaps this could permit 4 point type for the conspicuous portion of a notice if the rest of the notice is in 2 point type] boldface, wider spacing, or shading as set forth in (b)(2)(iii). We therefore suggest that the language in the example make it clear that these are factors that will be used in determining whether a notice is made reasonably understandable, and not safe harbored, and that in every case, constitute clear and conspicuous notice. In addition, we suggest that the language of (iii) be modified to read (iii) "...significance of the information contained in the notice if it meets (ii) and the bank uses:..."

The definition of "clear and conspicuous" seems to anticipate paper disclosures, since it does not also use examples for electronic display, such as online payday loan sites or on-site disclosures, such as posting at a check casher counter. Some payday loans are marketed online and fulfilled electronically through the ACH system without any personal contact with the borrower. In the sites visited by CFA, no privacy policy has been provided, although these sites request extensive personal financial information. Later in the rules, examples are given of delivering notices electronically. Clear definitions of what constitutes "clear and conspicuous" in the context of electronic disclosure would improve the rules.

"Collect" -- The proposed rule limits the definition of "collect" to information that is "organized or retrievable on a personally identifiable basis." The definition of "collect" should include information that could be tied or linked to an individual's identity at some point if paired with other data, even if it is not tied to an individual at the time it is collected. Existing technology allows for data thought not intended to be personally identifiable to be combined with other information which enables that data to be linked back to an individual at a later time.

"Customer and Consumer" -- We support the principle that the requirement for notice and the ability to opt out should simply be based on whether information regarding the individual, whether a "consumer" or "customer," as defined by the rule, is collected.

The obligation of notice and opt out should not be based on an institution's current intent not to share the data. An institution could avoid the obligations of the rule by simply not collecting the data or not sharing the data. A consumer should receive notice and be given the right to opt out if an institution keeps the data and could disclose it in the future.

The exceptions of who is covered by the definition of a consumer are not specific enough. In particular, the exception in (vi) is too broad. This exception states that "an individual is not a bank's consumer solely because the bank processes information about the individual..." We suggest modifying this example to state "an individual is not a bank's consumer solely because the bank processes and does not retain, or retains but does not share, reuse, or maintain the information about the consumer in a form which can be shared or reused..."

The draft rules define "customer relationship" as a continuing relationship that includes "having a credit account with you", but excludes isolated transactions such as cashing a check. The text of the example or the commentary to the regulation should clarify that a check cashing relationship can be a customer relationship. Some cash checkers issue an identification card or require payment of a membership fee. These are factors that might suggest an on-going customer relationship. The rules should clearly state that payday loans are included in "having a credit account" constituting a "customer relationship." Although a payday loan may appear to be an isolated transaction with the loan due and payable in full within a few days, in reality payday loan customers often renew, extend or maintain a series of loans. Lenders typically require extensive information disclosure from customers, such as recent bank statements, evidence of employment, and utility bills. When loans are extended, this documentation is not required. Therefore, the initial loan in actuality establishes an on-going relationship. A payday loan customer should be added to the examples in section (I)(2).

"Financial Institution" -- We support the ability of the Federal Trade Commission to implement privacy rules. The marketplace is changing, and many businesses long considered to be non-financial in nature, are offering products and services that are closely related to banking. All types of personal information, both financial and non-financial, is collected and used by these businesses in the course of dealing with consumers.

Section .4 Initial notice to consumers of privacy policies and practices required.

Privacy policies are not a substitute for privacy protections. We have already seen that FTC studies, as well as studies of the policies of health care web sites, that privacy policies and stated practices are not always followed.

The rule should ensure that institutions not bury disclosures in the fine print, or allow an institution to confuse its practices by making the privacy notice or policy unintelligible or misleading. Notices should be understandable and written in plain English.

Notice of privacy practices should always be provided before the collection of personal information. Allowing an institution to provide notice after data collection is begun means that the individual will not be allowed to opt out, or choose not to provide the information, or take his business elsewhere. The notice should be provided separately from other disclosure information.

There are some cases where a consumer will get no notice about the information sharing practices of an institution or be given the ability to opt out of that sharing of data. Consumers should be

warned that in many instances exceptions that allow an institution to avoid having to provide notice of its practice of sharing data with others, like those where third parties are used to service accounts. Consumers should also be told at the outset where an opt out does not have to be provided, such as when the institution has a joint marketing agreement with a third party.

The rules should include a general statement that institutions are required to use when an exception allows the institution to avoid notice and opt out. A statement merely stating that the institution will share information "as allowed to by law" is grossly inadequate. If these circumstances are not fully described, a consumer's ability to choose will be inhibited. There are other circumstances where a consumer will get notice, but not the ability to opt out. Consumers need to be informed of these situations as well.

Q. Notice where there is more than one party to an account.

Each account holder should have the ability to opt out of information sharing, since often there may be no way to separate out the information contained in the account by each party. Any party's objection to the sharing of the account information should be honored for the entire account. The institution has other opportunities to provide products and services to all of the account holders, such as through advertisements.

Q. Burden and methods of providing initial notice.

The initial notice should be provided in a way that is the least burdensome on consumers. For example, a consumer should not be required to make an additional trip to the institution to get a copy of the notice.

We urge regulators to require that an initial notice should be given concurrently with either the purchase of the product or service or when the relationship is established. Not only will this be less burdensome on those consumers who may not have any other contact with the institution, but it will also help consumers decide whether or not to do business with that institution. The notice should be provided in writing at the time of the initial contact between the consumer and the institution. In addition the notice should be distinct and not part of other information provided to consumers.

We are not persuaded by arguments of some in the financial services industry that providing notice to customers and other consumers about privacy policies will be too burdensome or costly. We are alarmed by recent claims that industry is claiming that providing disclosure will prove to be too burdensome, especially since the disclosure provision was touted as the landmark piece of "historic" privacy requirements. Institutions typically have ongoing correspondence with their customers. For example, many of the institutions covered by the rule aggressively market to their customers already.

A less burdensome alternative would be to adopt an opt in approach for information sharing. It would then be in the interest of the institution to convince their customers to allow personal data to

be shared. If the institution thought that providing notices would be too burdensome, it could simply choose not to do so and thereby not be allowed to share the consumer's personal information.

We support the proposed rule's requirement that electronic disclosure of privacy policies can only be provided when the transaction is conducted online and the consumer agrees to receive the notice online. This narrow provision for electronic disclosure should ensure that consumers doing business in person or through the mail are not deprived of privacy notices. The opt out form should only be used electronically if the transaction is being conducted online. In all cases, electronic notice, disclosure and opt-out forms should not be permitted for in-person transactions. The rule should also require that consumers be able to download and print the privacy notices and opt out forms. Further, where annual notices are required, the rule should require verification of receipt of the electronic message by the consumer. It is our understanding that the agencies are considering separate rules on electronic disclosures and any electronic disclosures contemplated by this rule should be subject to those regulations.

Q. Other situations where providing notice by mail is impracticable.

Unless the notice and opt out are provided to the consumer, the institution should not be allowed to share any information related to that individual. If notice by mail is impracticable, the institution should use other means to ensure that notice is sent. Because the mail is considered to be more reliable than other means of delivery, the institution should be required to verify that notice was received where an alternative method of delivery was used.

Section .5 Annual notice to customers required.

In some cases, an annual notice may not be adequate. Information required to get a loan or an insurance product is more detailed and personal than what a customer must provide to open a checking account. A customer should receive notice and be given the ability to opt out of information sharing each time a new product or service is purchased. At a minimum, the customer should get a warning that unless an opt out is exercised the new information provided to the institution can be shared.

Customers should have access to current policies, as well as to the policy that applies to them, especially if there are material changes in the policy. Institutions should have to abide by the last policy provided to the customer. An institution has the opportunity to provide a customer with a new notice prior to the timing of the annual notice, but should also provide a new opt out disclosure as well.

Q. Terminated accounts.

As long as the information is held by the institution, consumers, even those who have terminated their account, should be given notice. An alternative would be to assume that a consumer who has terminated their relationship with an institution has opted out of the sharing of their information.

At a minimum, a consumer terminating their relationship should be provided the opportunity to opt out at the time of termination and be told what will happen to their information. The institution must abide by the last decision made by the customer even after the end of the relationship.

If an institution decides to share more information than it has previously disclosed to a terminated customer, the institution should be required to give that customer a further opportunity to opt out before expanding the kind of sharing that will occur beyond that which was already disclosed to the customer.

Section .6 Information to be included in initial and annual notices of privacy policies and practices.

Congress intended that consumers use the notice provided by institutions to make decisions on whether to do business with a particular institution. It is too easy for some to provide notices in such a way that consumers could be confused. We recommend that the proposed rule include a basic format for notices so consumers can more easily compare policies. A standardized format will also be useful to the institutions as they draft their notices.

The notice should include how the information is collected, the sources of the information, and the purpose for which the information was collected and/or used. The notice should include a detailed description of the information that is collected and the affiliates and third parties with whom the information will be shared. General categories of information in these areas, as called for in the proposed rule, are inadequate. In some cases consumers may want more detailed information. For example, consumers should be able to access information on the specific companies that will get their information. This information will enable a consumer to check, for example, the various kinds of businesses a company that obtains their information is engaged in, or whether that company has been penalized for any privacy violations by any government agency. The purpose for which the information is being collected will also assist consumers making choices.

As we state above, unless consumers and customers are warned that in some instances their information can be shared without notice and opt out, the disclosure is inadequate. Banks should have to provide an explicit statement: "Where we have a joint agreement with a company or any party servicing your account, you will not be given notice and cannot tell us not to share your information with that company. We do not have to provide you the names of those companies."

Consumers may have different levels of comfort regarding information sharing, depending upon what types of information is shared. For the disclosure to be useful, it should describe the kind of information that will be provided. For example, the agency could help to move this marketplace toward further competition among financial institutions to respect their consumers' privacy rights if the required disclosure clearly set out specific categories of information and require the financial institutions to describe what kinds of information would be shared. In essence, we are suggesting that the agencies develop a "notice and score card" that would give consumers real and useful information about what would be shared. The financial institution would be expected to inform the consumer if they plan to share information with either their affiliates or third parties.

One way to do this would be to propose a notice that might say something like the following: "We are permitted by federal law to share this information about you either with companies we own or with other third parties who have a joint marketing arrangement with us. We can also share information with third parties unless you ask us not to do so. We plan on sharing your personal information from the following marked categories with affiliates (and a similar box for information we plan to share with third parties):

- The amount of your assets, or the type of assets you hold.
- Your mortgage balance.
- Your social security number.
- Biometric information such as your fingerprints.
- Your account balance.
- Your bank account number.
- Your credit card number, the amount of your highest balance, the amount of your current balance, the amount of your credit limit, the names of co-signers on your card, and also information about where and how often you use your card.
- Transaction History, including whether you use your ATM card for retail or other point-of-sale purposes.
- How much and the kinds of insurance you carry.
- Whether or not you have children; what are their ages and names.
- How often you use your home equity credit or other credit line, or for what kinds of purchases.
- Information you give to us to help you develop a financial plan.
- Information we have about your IRA, 401K, or retirement plan including the amount in your account or the types of retirement investments you hold.
- The fact that you have an account or loan with us.
- Your credit or risk score or other modeling that predicts either your purchasing behavior or propensity toward bankruptcy.
- Whether you have bounced a check or used an overdraft protection plan.
- How many types of products or services you have with us.

A similar list could be provided for the financial institution to provide information regarding their information sharing practices with third parties.

Section .7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.

Q. Opt out rights for joint accounts.

Any individual holding joint accounts should be able to opt out of information sharing for each account or type of relationship with the institution. However, once an individual in a joint account has opted out, that opt out should be valid for that entire account. The financial institution should not be able to require all holders of a joint account to opt out before the opt out is effective. Many

families divide the work of managing their finances, and a household or family unit in which one adult has opted out is highly likely to think this opt out is effective for the entire family. The regulation should clarify that an opt out with respect to an account applies to all information related to that account, not just the information about the individual who has opted out.

One aspect of the approach taken in this portion of the regulation is helpful. The regulation suggests that a consumer need opt out only once in order to affect all of the information a single financial institution has about that customer, even if the customer has multiple relationships with that institution. This is the right result, and we urge the agencies to maintain it in the face of potential industry opposition.

Q. 30 day opt out opportunity for notices sent by mail and examples for electronic transactions.

A 30 day opt out period is too short. Increasingly, banks have begun sending consumers their account statements and other materials on a rolling basis, although consumers may still desire to pay their bills at the end of the month. A 60 day opt out period makes more sense, since it will include at least one full monthly cycle. Of course, the consumer must still be provided with an ongoing ability to opt out at any time. It is important that there be some verification that the consumer actually received the notice prior to tolling the 60 day period.

Section .8 Form and method of providing opt out notice to consumers.

The format for the opt out should be determined by the agencies so that it is uniform. This will help avoid consumer confusion. We urge the agencies to develop model forms for use by institutions. These model forms may also be helpful in educating consumers about how institutions share their personal data, when such sharing is allowed by law, and under what circumstances consumers have the ability to stop the sharing of their information.

Q. Specificity of timing requirements.

The ability to exercise an opt out should be provided prior to the consumer or customer providing any information that could be shared. At a minimum, information should not be allowed to be shared prior to allowing the consumer to exercise the option to opt out.

An institution should not be able to apply a new privacy policy to data collected under an old policy. If privacy practices change, the consumer should be provided with the new notice and given the ability to opt out. Information should not be allowed to be shared unless the consumer is given those disclosures and has had an opportunity to respond.

Q. Burden, methods of delivering, and numbers of opt out notices.

Consumers should be allowed to opt out via mail, e-mail, Internet websites or by phone. If a consumer chooses to opt out by mail a form should be provided, but any wording in a correspondence indicating that the consumer chooses to opt out should be honored. Any method available for a consumer to communicate with an institution should be considered an appropriate method for exercising the opt out. The final rule should make clear that no institution can impose unduly burdensome opt out notification restrictions on consumers. In particular, the agencies should strictly limit the amount of personal information -- such as social security numbers and account numbers and unlisted phone numbers, required to be collected for an opt out.

Section .9 Exception to opt out requirements for service providers and joint marketing.

The exceptions to the opt out requirements provided in GLB allow for virtually unfettered sharing of personal information between institutions and third parties. We appreciate the need to share information under certain circumstances, like the printing of checks, or for underwriting purposes. At the same time we recognize that those purposes are limited. In most of these situations the consumer can reasonably expect that their information will be needed to conduct that part of the transaction. What is not expected is that the information used for that initial or primary purpose will then be kept and used for other purposes, completely unrelated to the purpose for which the information was originally given.

We note that Memberworks, the company that was subject to a suit filed by the Minnesota Attorney General, has agreements with most of the largest national banks in the country. Under the exceptions to the notice and opt out provisions, consumers would not have to be told, or given the ability to opt out, of their institution's sharing of personal information with Memberworks or companies like Memberworks. There is no way for consumers to know of the relationship with a company that they may not want to have their personal data shared with.

Q. Credit scoring models.

Aggregated data is less of a privacy concern than the sharing of personally identifiable information. At a minimum, consumers should receive notice that their data will be aggregated. It must be clear that the information will not be in a form that is personally identifiable or can be traced back to a particular individual.

Q. Additional disclosure requirements for service providers.

An institution should be required to provide the names of their service providers to customers.

Q. Other protections of a consumer's financial privacy under the joint agreement exception.

The regulation should comment on whether the rules should require the financial institution to take steps to assure that a product being jointly marketed with others does not present undue risk for the institution. We strongly support additional action in this area. We believe that a financial

institution should, before entering into a joint marketing agreement, examine the product, the value of that product to consumers, its sales, marketing and business practices related to both the sale of the product and the delivery of benefits under that product. A bank that lends its name to a low-quality product takes a risk with its reputation, and exposes itself to liability.

We also strongly support additional requirements to insure that not only is the financial institution's sponsorship evident from the marketing, but that the marketing clearly shows that the financial institution is not offering the product. The bank should also note that it does not stand behind the product in the event of a dispute between the consumer and the third-party marketer. This is very important because consumers often receive third-party marketing material which is designed to suggest that the product is being sold directly by the financial institution rather than by an unaffiliated third party who will provide the consumer's only source of redress in the event of a dispute.

Section _10 Exceptions to the notice and opt out requirements for processing and servicing transactions.

The agencies should define "processing and servicing transactions" so it is clear to consumers what sorts of information sharing will be allowed and for what purpose. The use of information to market products to a consumer is clearly in no way part of servicing an account.

The agencies should construct exceptions very narrowly. All exceptions should be limited with no further use allowed. Sharing of information under an exception should be disclosed to the consumer. Any additional exceptions should not be allowed

Section _.11 Other exceptions to the notice and opt out requirements.

We have deep concerns about the exceptions for consent in sections ____ . 11. Any such consent must be presented in a way that makes it clear that the consent is not required to move forward in the transaction, and that the consumer may withhold that consent. In section A(2)(ii) the exception for actual or potential fraud, unauthorized transactions, claims and other liabilities should be tightened to make it clear that this exception does not give broad ability to snoop in the consumers payment history. To do so, the language should be tightened to read, "to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liabilities of the consumer or the financial institution."

Finally, the consent exception in section ____ .11 A(1) is an enormous exception which could essentially swallow the rule. Under this consent exception, the consumer would get no notices or disclosures or even a reminder of a consumer's ability to opt out once there has been a "consent." We believe it would be contrary to the purposes of spirit of GLB to permit a single broad consent before the customer has received the information about what is at stake or even the information sharing policy of the institution. In addition, a broad consent customer loophole is likely to invite customer dissatisfaction or even litigation. A separate signature or a separate web page will not

be sufficient to resolve this problem. In addition, any solicitation for consent should contain a very clear statement that the consent is not required. The institution should also be required to test customer understanding of the nature and meaning of the consent.

The danger with consent clauses is that they can be cleverly drafted to give companies almost a free hand to process data as they wish. In practice, consumers are often forced to accept the companies' terms or otherwise lose the opportunity to do business with the company (or many times with any other company) at all.

Section .12 Limits on redisclosure and reuse of information.

Q. Third party compliance with limits on redisclosure of information.

We support the principle that requires that the limits on reuse and sharing follow with the information.

The use of personal information by a third party should not be allowed outside the scope of the purpose for which the information was originally provided. Such use may not be subject to the initial notice requirements and a consumer should be given the opportunity to make the decision to opt out of such uses. Such practices could open the door for abusive behavior.

Section .13 Limits on sharing of account number information for marketing purposes.

The limits on sharing account number information are easily overcome. An institution can provide all the data necessary to market to a consumer, except the actual account information. Once the sale is made, the marketer could easily access the account number data from the institution to "service" the new account.

The question to section ____ .13 asks whether there should be a consent exception to the general prohibition on disclosure of an account number. We strongly urge that there be no such consent loophole on this key prohibition. The agencies also seek comment on whether section 5 or 2(d) prohibit the disclosure by a financial institution to a marketing firm of encrypted account numbers if the encryption key is not provided. We believe that this section does prohibit providing account numbers whether or not they are encrypted. Those numbers have no value to the third party if they are encrypted and the encryption key is not provided. For this reason, this risk should not be taken.

Section .14 Protection of Fair Credit Reporting Act.

The regulators should clarify that the FCRA does not prevent states from adopting stronger privacy protections.

Section .15. Relation to State laws.

State efforts and new legislation are needed to provide protections of choice and access and to close the loopholes opened in the GLB, through which financial institutions can avoid providing consumer choice and, in some cases, avoid providing notice. Clearly the intent of Congress to allow states to adopt stronger laws.

Other issues.

The proposed rule should address these areas:

- Clarify that these rules apply to online transactions conducted between financial institutions and consumers.
- Include a section on how an institution's control over consumer privacy may lead to an anticompetitive effect in the marketplace in the report required to be sent to Congress.
- Specify enforcement mechanisms, including audit procedures, to ensure that institutions comply with their privacy policies.
- Ensure that institutions draft notices in plain English so that consumers can understand them.
- Use the authority granted in Section 501 and 503 to allow consumers to access data collected about them and to be able to correct wrong information. If regulators do not allow consumers the ability to access and correct data, at a minimum, a notice telling consumers that they have no right to obtain access to or to correct personal information held by institutions and disclosed to their affiliates and to third parties. Institutions should also be required to disclose to consumers why access and correction rights are not provided.

CONCLUSION

Consumers should have the right to be fully and meaningfully informed about an institution's practices. Consumers should be able to choose to say "no" to the sharing or use of their information for purposes other than for what the information was originally provided. Consumers should have access to the information collected about them and be given a reasonable opportunity to correct it if it is wrong. In addition to full notice, access, and control, a strong enforcement provision is needed to ensure that privacy protections are provided.

Respectfully Submitted,

Frank Torres
Rob Schneider
Gail Hillebrand
Shelley Curran
Consumers Union
1666 Connecticut Avenue, NW Suite 310
Washington, DC 20009

(202) 462-6262

Travis Plunkett
Jean Ann Fox
Consumer Federation of America
1424 16th Street, NW Suite 604
Washington, DC 20036
(202) 387-6121

Edmund Mierzwinski
US Public Interest Research Group
218 D Street, SE
Washington, DC 20003
(202) 546-9707