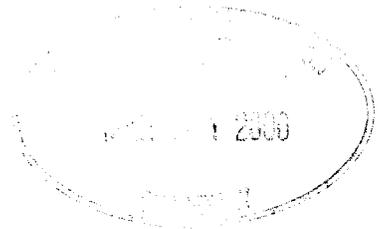




1717  
Pennsylvania  
Avenue, N.W.,  
Suite 500  
Washington,  
D.C. 20006

202-974-1000

info@efscouncil.org



March 31, 2000

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

Jennifer J. Johnson  
Secretary  
Board of Governors of the Federal Reserve System  
20th and C Streets, N.W.  
Washington, DC 20551

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

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

Becky Baker  
Secretary of the Board  
National Credit Union Administration  
1775 Duke Street  
Alexandria, VA 22314-3428

Donald S. Clark, Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

Jonathan G. Katz  
Secretary  
Securities and Exchange Commission  
450 5th Street, N.W.  
Washington, DC 20549-0609  
RE: File No. S7-6-00

Jack Chesson  
Federal and International Relations Office  
National Association of Insurance  
Commissioners  
444 N. Capitol Street, N.W.  
Suite 701  
Washington, DC 20001

Re: Proposed Rules Implementing the Privacy Provisions of the Gramm-  
Leach-Bliley Act

Dear Ladies and Gentlemen:

The Electronic Financial Services Council (the "EFSC"), which represents a wide variety of companies that deliver financial services over the Internet, appreciates the opportunity to submit its views on the proposed rules implementing Subtitle A of Title V (the "Privacy Provisions") of the Gramm-Leach-Bliley Act, Pub. L. 106-102 (the "Act"). The Office of the



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 2

Comptroller of the Currency (“OCC”), the Board of Governors of the Federal Reserve System (“Board”), the Federal Deposit Insurance Corporation (“FDIC”), the Office of Thrift Supervision (“OTS”), the National Credit Union Administration (“NCUA”), the Federal Trade Commission (“FTC”), and the Securities and Exchange Commission (“SEC”) have all published proposed rules that would implement the Privacy Provisions.<sup>1</sup> In addition, the National Association of Insurance Commissioners (“NAIC”) is considering how its members can prepare rules implementing the Privacy Provisions with respect to state-regulated insurers, consistent with those already proposed for other types of financial institutions. Our members are not only banks, thrifts, credit unions, insurance companies and broker/dealers, but also technology companies that are subject to FTC regulation for privacy purposes (if they are subject to the Privacy Provisions at all). We therefore believe it is appropriate for us to comment to all of these agencies and organizations (collectively, the “Agencies”) about the Privacy Provisions’ impact on providers of financial services over the Internet. Because the versions of the proposed rule (collectively, the “Proposed Rule”) published so far are very similar to one another, and because we feel strongly that the versions of the final rule (collectively, the “Final Rule”) the Agencies produce should be as close to identical as possible, we think it appropriate to submit our comments in the form of a letter jointly addressed to all of the Agencies.<sup>2</sup>

Our comments address those topics raised by the Proposed Rule which the EFSC believes have the most significant impact upon the electronic delivery of financial services. Privacy considerations are of ever-increasing importance to consumers, especially in the context of the Internet. As pioneers of a new way of delivering financial services, our members keenly understand the need to set standards to respond to that consumer demand. Our comments reflect our strong commitment to setting standards that protect consumer privacy consistent with a workable legal and regulatory structure.

---

<sup>1</sup> Privacy of Consumer Financial Information, 65 Fed. Reg. 8770 (February 22, 2000) (OCC, Board, FDIC, OTS joint notice); Privacy of Consumer Financial Information, Requirements for Insurance, 65 Fed. Reg. 10,988 (March 1, 2000) (NCUA notice); Privacy of Consumer Financial Information, 65 Fed. Reg. 11,174 (March 1, 2000) (FTC notice); Privacy of Consumer Financial Information, 65 Fed. Reg. 12354 (March 8, 2000) (SEC notice).

<sup>2</sup> The Agencies’ versions of the Proposed Rule have virtually identical internal numbering, although they vary in their specific placement in the Code of Federal Regulations. Thus, for example, the Board’s version is 12 C.F.R. Part 216, while the FTC’s version is 16 C.F.R. Part 313, but 12 C.F.R. § 216.12(a)(1) is identical to 16 C.F.R. § 313.12(a)(1). In this letter, we would reference this section of the Proposed Rule as “Proposed § \_\_.12(a)(1).” Where the numbering of the Agencies’ versions differ, chiefly in Proposed § \_\_.3, we note them as “Proposed § \_\_.3(j)(1) (NCUA version (k)(1), SEC version (m)(1)).”



## EXECUTIVE SUMMARY

A summary of our major comments to the Proposed Rule may be helpful, given the number of Internet-related issues that the Proposed Rule raises, the complexity of those issues, and the consequent length of this letter. A complete explanation of each comment will follow.

On a procedural level, we note at the outset the vital need for consistency among the various regulators. The nature of the Internet requires uniformity among federal and state regulations in order to provide a common reference point for all applicable businesses and to ensure that individuals can rely upon a single, predictable, comprehensible standard of privacy when online. Our substantive comments fall into three major categories: (1) the need to clarify the scope and applicability of the Privacy Provisions by refining crucial regulatory definitions; (2) the need to take into account the special notice, opt-out, distribution and reuse situation of the typical Internet-based company; and (3) the need to provide guidance on the scope of companies' legal responsibilities under the Privacy Provisions.

### *Crucial Definitions Need Refinement*

For many businesses, the applicability of the Privacy Provisions is vague at best, because key terms and phrases used in the Proposed Rule are not adequately defined or explained. Definitional issues include:

- Activities deemed “financial in nature”: Not all activities in which financial institutions engage are automatically “financial in nature,” and the Final Rule should explicitly enumerate the activities that are covered. The guidance provided to date by the Board in the context of permissible activities for financial holding companies does not offer the specificity needed for workable privacy regulations.
- Need for uniformity in the list of activities “financial in nature” for purposes of the Privacy Provisions: When establishing a list of activities “financial in nature,” and of those activities that are excepted from the definition, it is imperative that the Agencies coordinate their actions, producing a single, uniform list that remains uniform going forward in time.
- Intent behind the phrase “significantly engaged in financial activities”: If any of the Agencies intend to adopt a *de minimis* standard, they should unanimously determine the appropriate level of activity. If the Agencies merely intend to restate that certain



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 4

activities could bring a business within the scope of the Proposed Rule, we urge them to concentrate on producing an explicit list of covered activities.

- Nature of a “financial product or service”: In order for the Final Rule to be usable in business, the Agencies should provide certainty regarding both the term “financial” and the term “product or service.” Again, we urge the Agencies to accomplish this objective by providing a discrete list of “financial products or services.”
- Use of a product or service “for personal, family or household purposes”: In determining who constitutes a “consumer,” the Agencies should permit financial institutions to rely upon the reasonable representation of the putative consumer with regard to the intended use of the product or service.
- No responsibility for wholesale or passive provision of a financial product or service: Recognizing that many of the unique characteristics of Internet businesses do not raise the privacy concerns that the Proposed Rule is intended to address, the Agencies should exempt from the Final Rule entities that do not provide products or services to consumers either directly (*e.g.*, wholesalers, service providers) or actively (*e.g.*, software hosts).
- Scope of “continuing relationship”: Because what makes a consumer into a customer triggers significant new responsibilities, the Agencies should clarify when that transition occurs, either by listing the activities that create a continuing relationship, or by stating that transactions that impose no on-going legal responsibilities do not create continuing relationships.
- Alternative B definition of “nonpublic personal information” preferable to Alternative A: In the interests of a uniform, workable regulatory scheme, the Agencies should adopt Alternative B in the form proposed by the SEC.
- Time-frame of “nonpublic personal information”: In order to avoid unjust and unequal burdens, the Agencies should make clear that information a financial institution has collected from or about individuals who are no longer customers as of the effective date of the Privacy Provisions should not be covered by the Final Rule.
- Limitations on “personally identifiable financial information”: Even after adopting Alternative B, the Agencies should still clarify that only information directly linked to an identifiable individual is protected, that a financial institution may collect and disclose information lacking personal identifiers, and that a third party receiving personally



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 5

identifiable information may delete the personal identifiers and redisclose the information.

- Permissible type of “list, description or other grouping ... derived using personally identifiable financial information”: Unless a list, description or grouping of consumers can be “decoded” to obtain personally identifiable financial information, such generic information should fall outside the scope of the Final Rule.
- Parameters of “publicly available information”: In the interests of certainty and efficiency in the application of workable privacy standards to protect consumers, all of the Agencies should follow the lead of the SEC and define “publicly available information” as information that financial institutions “reasonably believe is lawfully made available to the general public[.]”
- What Internet sites qualify as “widely available media”: Widely available media should include Internet sites that an institution reasonably believes an individual could access from a publicly-available facility such as a computer in a public library, without that individual having to provide a password or pay a fee.
- Clarity of the term “affiliate”: Congress intended to allow companies to share information among affiliates. In order to make the term “affiliate” usable in practice, the Agencies should adopt the SEC’s more objective definition for the crucial term “control,” which actually may be more consumer-friendly than definitions in other versions of the Proposed Rule.

In general, the Agencies should adopt “bright-line” standards at the definitional level, so that companies clearly know whether and how to comply with the Final Rule and, equally important, so that consumers know what to expect when transacting business over the Internet. Clarifying these key definitions would be a major step forward in this effort.

*Notice, Opt-Out, Distribution and Reuse Requirements Need to Include Guidance Specifically Applicable to the Internet Context*

To effect the intent of Congress that the standards applicable to the delivery of privacy disclosures in “online” relationships be no more or less stringent than those required in an “off line” context, the Agencies should make the Proposed Rule more Internet-friendly in the following areas:



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 6

- Actual Notice: Several clarifications are essential in the interests of technology-neutrality and efficiency. First, a business should be allowed to provide the privacy policy to a consumer by any mode of delivery (*e.g.*, e-mail), provided that the consumer consents to such mode of delivery. Also, a privacy policy disclosure should be permitted to cover a range of Internet addresses or sub-addresses, provided that it is clear to the consumer which addresses or sub-addresses the disclosure covers. Similarly, a business should be permitted to use a single privacy policy disclosure for various products or services, provided that it is clear to the consumer which products or services the disclosure covers. Finally, a business should be permitted to utilize a link to a third-party service provider's site, provided that the effect is the same as if posted on its own site and legal liability remains with the original business.
- Co-Branded Products and Services: In the interests of consumer-friendliness, institutions offering co-branded products and services should be permitted to supply a single privacy policy notice, provided that the joint disclosure clearly and accurately describes each institution's policy.
- Joint Accounts: The Agencies should recognize by rule that in cases where persons establish joint accounts, institutions are permitted to provide a single privacy policy notice and a single opt-out. Moreover, the decision by one joint account holder should be binding upon the other joint account holders.
- Maximize the Efficiencies Created by Electronic Delivery of Notices: In order to avoid needless duplication that burdens business and annoys consumers, businesses must be able to track electronically to whom they have delivered privacy policy notices. Provided that consumers receive notice (but without an opt-out by consumers), the Agencies should explicitly endorse this efficient result in the Proposed Rule. The Agencies should not undermine the efficiencies thus achieved by requiring businesses to accept opt-outs at every point of contact with consumers.
- Establish Electronic "Reasonable Opportunity" Standards for Opt-Outs: Reasonable response times for electronic notices should be determined with respect to the method of delivery – the Internet – instead of the periods applicable for slower methods of delivery, such as the mail. We urge the Agencies to adopt three (3) days as a reasonable and appropriate standard for both consumers and customers.



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 7

- Permit Businesses to Take Maximum Advantage of Non-Marketing Outsource Opportunities: Businesses should be able to change outsource service providers without having to provide expensive change-in-terms privacy notices.
- Establish Reasonableness Standard for Consumer Consent: Businesses should be able to obtain consumer consent to information-sharing without having to meet unreasonably high disclosure standards.
- Give Institutions Receiving Information Flexibility in the Distribution and Use of Information They Receive: Businesses that receive information appropriately under the Privacy Provisions should be able to redisclose or use that information pursuant to any of the exceptions to the notice and opt-out rules.

*Guidance as to Legal Responsibility*

Finally, the Agencies should clarify several lingering questions regarding the allocation of legal responsibility in the Internet context:

- Responsibility for Third Party Use of Information: A financial institution should not be responsible under the Privacy Provisions for the breach of a confidentiality agreement by a third-party service provider.
- Effects of Overlapping Federal Requirements and Permissions: The Proposed Rule should be consistent with other rules that are currently applicable to certain aspects of information sharing (e.g., the statutes and Fair Credit Reporting Act). The Agencies should also clarify that the Proposed Rule does not reverse the rule of statutory interpretation that laws are not afforded extraterritorial effect unless specifically provided by Congress.
- Postpone Mandatory Compliance with the Privacy Provisions: Given the ambiguities surrounding the applicability of the act to many businesses, the practical realities of business production cycles for new products to be introduced in 2001 and the desire to avoid widespread non-compliance (despite good-faith efforts to comply) that could make the Privacy Provisions appear ineffectual in the eyes of consumers, the Agencies should not require compliance with the Privacy Provisions until November 13, 2001.

## COMMENTS ON THE PROPOSED RULE

The Agencies will undoubtedly receive many letters commenting exhaustively on the Proposed Rule. We do not think it useful to repeat that effort, particularly given that different agencies have solicited comments on different aspects of the Proposed Rule. Our concern is with the impact of the Proposed Rule on the Internet, and only some elements of the Proposed Rule have special significance to on-line providers of financial services. We have concentrated on these elements, noting the special significance of each issue to the Internet and suggesting solutions that would be particularly appropriate in that context.

### **Importance of Consistency Among Regulations**

We feel uniquely qualified to stress how important it is for the regulations implementing the Privacy Provisions to be consistent among all federal and state regulators. Electronic transactions cross over traditional regulatory boundaries with ease, and businesses regulated by all manner of government agencies compete over the Internet virtually on an equal footing. It would be intolerable if national banks, federal thrifts, state banks, broker/dealers, credit unions, insurance companies and non-chartered financial institutions were subject to privacy regulations that differed in any but the most trivial respects. Consumers who transact business over the Internet demand that companies respect their privacy and the confidentiality of their information. They would neither understand nor accept that their privacy is subject to different levels or specific forms of protection based upon the federal or state regulator of the business with which they deal. Such uneven regulatory effects would serve only to discredit and diminish the signal achievement of the Privacy Provisions: providing nationwide protection for consumer financial information. Congress recognized the importance of crafting a single rule applicable to all financial institutions, requiring the Agencies to

consult and coordinate ... for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities.

Pub. L. 106-102, § 504(a)(2). The Agencies have done an exceptional job of producing largely consistent and comparable regulations. Most of the specific comments we make below therefore apply to language that all of the Agencies have agreed upon. Where our comments apply to language not common to all of the Agencies, we note which language we think most appropriate for all of the Agencies to adopt. In every case, we think it crucially important for all of the



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 9

Agencies to agree about whether or not to adopt our recommendation, or to have the Final Rule reflect our comment.

### **Crucial Definitions Need Refinement**

It is vitally important for the Agencies to refine the definitions that determine the scope of the Privacy Provisions. Currently, the ambiguities in these definitions make it difficult for businesses to know whether they are subject to the Proposed Rule, and if so, to what degree. Under the Privacy Provisions, some businesses are financial institutions despite not being regulated by a banking, securities or insurance regulator -- in other words, some businesses are "financial institutions" exclusively because of their activities. Some of these businesses may still not be aware that the Proposed Rule applies to them. Companies that, unbeknownst to themselves, have become subject to regulations about which they had no notice and no opportunity to comment may be unable to comply. Even companies that are aware that aspects of their activities may be subject to the Privacy Provisions will be severely handicapped in commenting on the Proposed Rule or complying with the Final Rule unless they have a more specific statement of which aspects of their activities are contemplated to fall within the scope of the regulations' requirements. As you can appreciate, leaving such matters to speculation makes meaningful comment on the Proposed Rule very difficult.

*What is a financial institution (1): What is an activity "financial in nature"?*

The most important definition under the Proposed Rule, and the one most in need of clarification, is that of a "financial institution." Proposed § \_\_.3(j) (NCUA version (k), SEC version (m)). This definition determines the scope of the regulations: the Privacy Provisions apply to financial institutions, as well as to other persons that receive nonpublic personal information from financial institutions. Proposed § \_\_.1(b). The Proposed Rule defines a financial institution as "any institution the business of which is engaging in activities that are financial in nature as described in section 4(k) of the Bank Holding Company Act of 1956[.]" Proposed § \_\_.3(j)(1) (NCUA version (k)(1), SEC version (m)(1)). Section 4(k) of the Bank Holding Company Act permits a financial holding company to engage in any activity that:

the Board determines ... (by regulation or order) (A) to be financial in nature or incidental to such financial activity; or (B) is complementary to a financial activity and does not pose a substantial risk to the safety or soundness of depository institutions or the financial system generally[.]



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 10

12 U.S.C. 1843k(k)(1). Financial activities include, not only those specified in Section 4(k), *see* 12 U.S.C. 1843k(k)(4)(A)-(E), but also those activities that:

the Board has determined, by order or regulation that is in effect on the date of the enactment of the Gramm-Leach-Bliley Act, to be so closely related to banking or managing or controlling banks as to be a proper incident thereto (subject to the same terms and conditions contained in such order or regulation, unless modified by the Board),

12 U.S.C. 1843k(k)(4)(F), as well as those activities that the Board has determined by Board regulation or interpretation to be usual in connection with the transaction of banking or other financial operations abroad. 12 U.S.C. 1843k(k)(4)(G).

Given the special role that this definition -- taken almost verbatim from § 509(3) of the Act -- assigns to the Board, we acknowledge that the Agencies have limited freedom to resolve this ambiguity by coordinated rulemaking. For this reason, we wrote to the Board, in a letter dated March 6, 2000 (attached), asking for clarification of what constitutes an activity “financial in nature” for purposes of the Privacy Provisions. The Board issued an Interim Rule on March 10, 2000, which provided a broad outline of activities permissible for a financial holding company under the Act. This Interim Rule goes some way towards clarifying what activities are financial in nature. For example, it specifies which of the Board’s many rulings in effect on November 12, 1999 are to be taken into account in defining activities financial in nature. *See* Interim 12 C.F.R. § 225.86(a)(2). But the Interim Rule still is not specific enough to permit potentially affected companies to know which of their activities might be subject to the Privacy Provisions.

The Interim Rule refers to specific sections of Regulations Y and K as part of the definition of an activity financial in nature. *See* Interim 12 C.F.R. § 225.86(a)(1), (b)(1). But these regulations do not provide adequate guidance for businesses to determine whether they are subject to the Proposed Rule. For example, Regulation Y permits the subsidiary of a bank holding company to engage in specified “data processing” activities, defined as:

- (i) Providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if —
  - (A) the data to be processed or furnished are financial, banking, or economic;  
and

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 11

(B) The hardware provided in connection therewith is offered only in conjunction with software designed and marketed for the processing and transmission of financial, banking, or economic data, and where the general purpose hardware does not constitute more than 30 percent of the cost of any packaged offering.

(ii) A company conducting data processing and data transmission activities may conduct data processing and data transmission activities not described [above] if the total annual revenue derived from those activities does not exceed 30 percent of the company's total annual revenues derived from data processing and data transmission activities.

12 C.F.R. 225.28(b)(14). Does this mean that *any* processing of “financial, banking or economic” data is a financial activity? That *any transmission* of such data is a financial activity? That providing *software* intended to process such data is a financial activity? If so, then virtually every Internet portal, every Internet search engine, every Internet news provider and every major software manufacturer would appear to be a financial institution. If not, then what fraction of such businesses are financial institutions? Only those whose non-financial data processing and data transmission activities generate more than 30% of the businesses’ total annual revenues? Does this mean that a small software manufacturer with two product lines, one of which is financial, is a financial institution, while a large software manufacturer with forty product lines, ten of which are financial, may not be? And if this is the test, how can an Internet service provider calculate the portion of its annual revenues that flow from the transmission of financial information? As this one example should show clearly, Regulation Y and Regulation K are inadequate as stand-alone definitions of what constitutes an activity “financial in nature.” Either they are overbroad, or they are unsupportably vague.

*What is a financial institution (2): List of Activities Financial in Nature, Developed According to Established Principles, is Needed.*

As we stated in our letter of March 6, the solution to this problem is to create a clear, definitive list of activities that are financial in nature. If the Board wishes, it can establish such a list for all the purposes of the Act, but that is not our primary concern. Rather, we urge the Agencies to work together to establish a list of activities that are financial in nature specifically for the purpose of the Privacy Provisions. Such a list, identical for all of the Agencies, would establish firmly the scope of the Proposed Rule. The Agencies should establish principles to govern the creation of this list. We understand that the Board is bound by statute to take into account certain specific considerations in defining an activity “financial in nature or incidental to a financial activity” for Bank Holding Company Act purposes. 12 U.S.C. 1843(k)(3). However, not every activity in which a financial holding company may engage is appropriately within the



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 12

scope of the privacy regulations. This being the case, the Agencies may want to except certain activities determined by the Board to be “financial in nature” from the scope of the Privacy Provisions.

In establishing this list and making these exceptions, the Agencies will need to act pursuant to a consistent set of standards. These standards will help the Agencies determine which activities are primary financial activities, appropriately subject to a rule protecting financial privacy, and which merely facilitate financial activities. An activity that involves taking an application, or obtaining information directly from a consumer, or offering a product or service, would appear to be a “primary” activity. By contrast, an activity that merely facilitates such a primary activity, and that can also facilitate non-financial activities, would not appear to be the proper subject of the Proposed Rule. Providers of such facilitating activities include certification authorities for digital signatures, computer software and hardware manufacturers and distributors, Internet portals, Internet search engines, and cable or wireless transmission companies.<sup>3</sup> Such companies undertake activities that facilitate financial activities but that would not appropriately be described as financial activities themselves, at least not for privacy purposes. It may be that financial institutions using these facilities should require them by contract to respect the privacy of information which the financial institution entrusts to them. But to define companies engaging in facilitative activities as “financial institutions” *per se* would stretch the meaning of those words beyond what we believe the authors of the Act could reasonably have intended.

Whatever is specifically included in the list of activities financial in nature, it is important that this list, to the extent possible, avoid vague catch-all phrases that give no notice to businesses that they may be “financial institutions” under the Privacy Provisions. If possible, the activities should be defined by reference to well-known lines of business, so that the list does not inadvertently multiply definitions. For example, if certain real-estate related activities are included in the list of activities “financial in nature,” as 12 C.F.R. § 225.28(b)(2) and Footnote 4 to the FTC’s version of the Proposed Rule suggest, the list should define those activities by

---

<sup>3</sup> Contrast a transmission company with one that stores information for subsequent transmission, an activity that would appear to come much closer to being a financial activity. The essence of a utility-like communications facility -- as a great deal of Internet activity is -- lies in its automatic transmission of information. The caller or the e-mail sender is in control of what message is being sent, when, how and to whom. It is as instantaneous as technology can make possible. If an institution stores information for subsequent transmission, by contrast, it is acting less like a utility and more like a researcher or an information broker. And if the information it is storing for future transmission is financial information, the institution is acting more like a financial institution. We urge the Agencies to adopt this distinction, which would be particularly useful in determining who in the Internet context has responsibilities under the Privacy Provisions.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 13

reference to the specific activities covered, such as: “provision of title search services,” “provision of title insurance,” “rendering of credit reports,” “provision of appraisals,” “provision of mortgage insurance,” and so forth. The list should be exhaustive, so that any activity not specified is excluded from the definition and from the scope of the privacy provisions.

This list must be the same for all of the Agencies. It would be unacceptable if, for example, a member bank of the Federal Reserve System were subject to privacy disclosure obligations in connection with providing appraisals, but a federal credit union were not, because the Board’s list of covered activities included “appraisals,” while that of the NCUA did not. To preserve fair competition, and to minimize consumer confusion, it is important to maintain a level playing field, with all companies providing like services treated alike for the purpose of compliance with the privacy rules. It is also important for this level playing field to be preserved into the future. If the Board includes a new activity as one “financial in nature” for the general purposes of the Act, the Agencies should refrain from adding that activity to the list of activities financial in nature for purposes of the Privacy Provisions until there is unanimous consent among the Agencies to do so. Only by the creation and maintenance of such a uniform list will the scope of the Privacy Provisions be both clearly and appropriately applicable.

*What is a financial institution (3): What does it mean to be “significantly engaged in financial activities”?*

Even with such a list, the definition of a financial institution under the Proposed Rule needs significant clarification. The FTC version’s attempt to define the category of “financial institution,” in particular, creates uncertainty, rather than eliminating it. *See* 65 Fed. Reg. 11,190 (Proposed § \_\_.3(j)(1), (2), (3)). In the FTC version of the Proposed Rule, an entity is a financial institution, according to the example, “if it is significantly engaged in financial activities, such as a retailer that extends credit by issuing its own credit card directly to consumers.” *Id.* (Proposed § \_\_.3(j)(2)). This suggests that the FTC wishes to adopt a *de minimis* standard, in which a finance company that made 200,000 commercial loans and 1000 loans to individuals in a calendar year might not be a financial institution because it was not “significantly engaged” in financial activities relating to individuals. The FTC’s commentary to the quoted language of the Proposed Rule, however, states that “[t]hus, a retail business that issues its own credit card directly to consumers is a financial institution engaged in the extension of credit, but a retail business that merely establishes lay-away or deferred payment plans is not a financial institution.” 65 Fed. Reg. 11,176 - 11,177. This language suggests nothing about a *de minimis* rule and makes a distinction between providing different kinds of credit for purposes of the Act, which is reflected nowhere in the FTC’s or any other Agency’s version of the Proposed Rule.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 14

We urge the Agencies to determine unanimously whether they are prepared to adopt a *de minimis* standard for the level of financial activities that makes a business a financial institution, as the FTC version's use of the phrase "significantly engaged" suggests, or whether the FTC's version is merely restating that certain activities are "financial in nature" for purposes of the Proposed Rule, as the commentary suggests. If the Agencies are prepared to adopt a *de minimis* standard, we urge them to establish the *de minimis* level explicitly, permitting our hypothetical finance company mentioned above to know whether or not it is "significantly" engaged in financial activities. If the FTC is merely restating that certain activities bring a business within the scope of the Proposed Rule (e.g., merchant credit cards are covered and lay-away plans are not), we urge it not to use the ambiguous phrase "significantly engaged in financial activities," but rather to take the opportunity, together with the other Agencies, to specify those activities that a business *per se* becomes a financial institution by engaging in.

*What is a financial institution (4): What is a "financial product or service"?*

In many respects, what constitutes a "financial product or service" is inextricable from who is a "financial institution." The definitions are very similar. The proposed regulations define a financial product or service as "any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act of 1956[.]" Proposed § \_\_.3(k)(1) (NCUA version (l)(1), SEC version (p)(1)). Like the definition of "financial institution," this refers to a broad but ill-defined category, providing no certainty in determining what is covered by the Proposed Rule. And, as we suggested above, we urge the Agencies to resolve this lack of certainty by adopting a list of those products or services that are "financial," in order to establish the scope of the Proposed Rule. A bright line dividing financial from non-financial products and services would permit businesses to offer both, confident that they could provide non-financial products and services outside the scope of the Proposed Rule. We have suggested two such bright lines above: financial products or services for purposes of the Privacy Provisions are those that an institution provides directly to consumers; or financial products or services for purposes of the Privacy Provisions are those that are primarily financial, rather than merely facilitative of financial and non-financial services.

It is important not only to have certainty about when something is "financial," but also about when something is a "product or service" for purposes of the Proposed Rule. Not every facility provided to a consumer to assist in a financial decision would appear to us to be appropriately designated as a financial service subject to the regulation. For instance, if a web site provides consumers with a mortgage calculator or stock quotes, but does not charge for the



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 15

use of the facility or retain any information regarding the consumer, should that facility be included within the regulation's definition of financial product or service? It may well be that providers of such free facilities will want to provide the public with privacy assurances, but to the extent that these activities are subjected to regulatory requirements, the legal cost of assuring on-going compliance with privacy rules may have a chilling effect on the offering of such free facilities. The Agencies will never know what free facilities were not offered as a result.

*When does a person obtain a product or service "for personal, family or household purposes"?*

Another definition that requires clarification is that of a "consumer." The Proposed Rule states that an individual who obtains a financial product or service "that is to be used primarily for personal, family or household purposes" is a consumer. Proposed § \_\_.3(e)(1) (SEC version (g)(1)). Products or services delivered over the Internet, however, are not always self-evidently for personal, family or household purposes -- such as accounting software, bill-paying services or investment advice. We urge the Agencies to state that a financial institution may rely on the reasonable representation of a consumer as to the use to which a product or service will be put, for purposes of compliance with the Privacy Provisions.

*Does a person "obtain" a financial product or service from a wholesale or passive provider?*

An additional aspect of the definition of a consumer that could be clarified concerns whom the consumer obtains the financial product or service from. A wholesale provider of financial products or services may be said to provide them to consumers, but because the provision is indirect the wholesaler may have no knowledge of the consumer and no contact with the consumer. In such a situation, there may be no compelling reason for the wholesaler to consider compliance with the Privacy Provisions, so long as the wholesaler does not receive any nonpublic personal information concerning the consumer. From our experience of Internet financial services, we can think of numerous examples, such as the provision of financial accounting software -- purchasers of which should not be considered consumers with respect to the wholesaler unless the wholesaler takes registration or warranty information from the consumers.

Besides wholesale providers of services, an additional category of financial services providers delivers services to consumers only indirectly. For instance, an appraisal service may be hired by a lender to prepare a property valuation, and such service will be paid for by a consumer, yet the appraisal company has contact only with the lender. While the lender might be

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 16

expected to bind the ancillary service provider by contract to respect the privacy policies of the lender vis-a-vis its customers, it is hard to understand how the appraiser would disclose its privacy policy to the consumer of its privacy policy, since it would ordinarily not have direct contact with the consumer. In financing a home, there are a number of such ancillary service providers. The proliferation of privacy notices which the consumer would receive if they were all obligated to provide notices could be confusing to a consumer, who viewed himself as a customer of the lender, not the lender's vendors.

A final category of company that does not actively provide financial services to consumers also deserves to be free from the requirements of the Proposed Rule, namely those companies that host software that consumers can access on the Internet. Such companies do not have any interaction with the consumer, and are better analogized to software vendors whose products are available at retail outlets. These companies are simply using the Internet as a distribution channel for their software, as contrasted with companies that engage in on-going interactive financial relationships with consumers over the Internet.

Again with the intention of creating regulatory certainty, we urge the Agencies to state that an individual is a consumer only with respect to those financial institutions to which the individual directly provides nonpublic personal information.

*What constitutes a "continuing relationship" with a consumer?*

Another definition which we would like the Agencies to clarify is that of a "customer" of a financial institution. The Proposed Rule defines a customer by reference to a "customer relationship," which in turn is defined as "a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer[.]" Proposed § \_\_.3(h), (i)(1) (NCUA version (i), (j)(1), SEC version (k), (m)(1)). Although the definition contains numerous examples, it does not make clear what constitutes a "continuing relationship."

Specifically, obtaining a financial product or service in an "isolated transaction such as" using an ATM, cashing a check or making a wire transfer does not establish a customer relationship. Proposed § \_\_.3(i)(2)(ii)(A) (NCUA version (j)(2)(ii)(A), SEC version (k)(2)(ii)(A)). At the same time, purchasing an insurance product or obtaining advisory services for a fee *per se* establishes such a customer relationship, presumably even if the insurance product or advisory service is obtained in an isolated transaction. Proposed § \_\_.3(i)(2)(i)(B), (G) (NCUA version (j)(2)(i)(B), (G), SEC version (k)(2)(i)(B), (G)). This suggests, either that the Agencies regard *certain* isolated transactions as not creating a customer relationship, or that the Agencies understand the meaning of an "isolated" transaction in such a way as to exclude a

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 17

one-time purchase of an insurance product or of investment advice. By not specifying which of these two possibilities they embrace, however, the Agencies create uncertainty as to precisely when an ordinary consumer becomes a customer of a financial institution. For example, would a purchaser of financial software be considered a consumer, given that he or she obtained the software in an isolated (*i.e.*, one-time) transaction? Or would such a purchaser be considered a customer, given that the software would be of at least as much on-going value to the purchaser as a piece of investment advice?

In the interest of regulatory clarity, we urge the Agencies to take one of two courses. They could list the transactions that do not create a customer relationship, stating whether the provision of software for consumer use does or does not, rather than using “such as” language that leaves this crucial question up to individual businesses with varying appetites for litigation risk and varying concern for consumer needs. Or the Agencies could define what they mean by an “isolated” transaction rather than merely providing examples. Defining an isolated transaction as one that does not create an on-going legal relationship (separate from product liability and warranty responsibilities) upon the financial institution with relation to the consumer would appear to encompass the Agencies’ examples, while providing enough guidance to allow businesses not covered by any of the Agencies’ specific examples to know how to comply.

*What is “nonpublic personal information”? Alternative B is preferable to Alternative A.*

Another definition crucial to determining the scope of the Proposed Rule is that of “nonpublic personal information.” The difficulty of producing a satisfactory definition of the term is clear from the fact that the Agencies are unable to decide unanimously between two alternative definitions. The NCUA version includes only the alternative labeled “Alternative A” by other Agencies. The Board version and the SEC version include only “Alternative B.” The versions of the OCC, FDIC, OTS and FTC include both. The consistency and comparability required by the Privacy Provisions are impossible to achieve if one of the key operational definitions of the regulations is not identical for all of the Agencies. Given the importance of having a uniform rule that applies in the same way to all financial institutions, whether chartered or unchartered, depository or non-depository, and given the support Alternative B already has, we think that all of the Agencies should adopt Alternative B in the form proposed by the SEC, and discussed in greater detail below.

In addition to ensuring consistency and comparability, the universal adoption of Alternative B will result in a far more workable regulatory scheme. As noted in the commentaries to the banking agencies’ and the FTC’s versions of the Proposed Rule, Alternative A would greatly expand the category of nonpublic personal information. 65 Fed. Reg. 8773,



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 18

11,177-78. While it is undeniable that this would increase the scope of the Proposed Rule, this is not the main reason we oppose the use of Alternative A. Businesses can deal with rules that apply broadly, so long as it is easy to determine just how broadly they apply. But this is exceptionally difficult to do under Alternative A. Under Alternative A, nonpublic personal information does not include “publicly available information.” Proposed § \_\_.3(n)(1)(i), (o)(1)(iii) (NCUA version (n)(1)(i), (p)(1)(iii)). Publicly available information, however, includes only information that is “obtained from” government records, widely distributed media, or government-required disclosures. Proposed § \_\_.3(p)(1) (NCUA version (q)(1)). This suggests that information will avoid the definition of Alternative A only if the financial institution actually obtains it from a qualifying public source and, more importantly, can show that it did so. This, in turn, requires that a financial institution keep track of not only the information it obtains but also the source of each piece of information. If a financial institution cannot document where it originally obtained a piece of information, it cannot determine whether the Proposed Rule applies to that information by consulting records in the public domain to see if the information is publicly available.

In the absence of virtually error-free record-keeping, therefore, Alternative A would keep a financial institution in a near-permanent state of uncertainty as to the usability of its own records. It may be argued that uncertainty breeds prudence, and indeed a prudent financial institution in such a situation could well decide not to distribute most information because of this uncertainty. But institutions not concerned with legal compliance would undoubtedly seek to exploit this uncertainty rather than respecting it, leading to a situation where businesses seeking to comply with the law would be penalized for that spirit of compliance by having to compete on unequal terms with their noncompliant competitors. No one profits from such a game of regulatory “chicken” except scofflaws and class-action litigators.

*Clarifying the Alternative B definition of “nonpublic personal information” (1): How long ago can the institution have obtained information, and still have that information be subject to the Privacy Provisions?*

Even if the Agencies agree unanimously to adopt Alternative B, we urge them to sharpen its definition of nonpublic personal information. The most important single clarification would specify that the time frame covered by the Privacy Provisions for all purposes is from the effective date of the Privacy Provisions forward. The Proposed Rule defines nonpublic personal information primarily as “personally identifiable financial information,” which in turn is defined without reference to any time frame:

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 19

*Personally identifiable financial information* means any information:

- (i) Provided by a consumer to you to obtain a financial product or service from you;
- (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
- (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

Proposed § \_\_.3(o)(1), (SEC version (v)(1)). The language suggests that any information that a consumer has *ever* provided, or that has *ever* resulted from a consumer transaction, or that an institution has *ever* obtained about a consumer, is covered by the Privacy Provisions.<sup>4</sup> If this were true, then as of the effective date of the Privacy Provisions every piece of information about a consumer ever collected by every financial institution would be subject to the restrictions of the Privacy Provisions. In addition, every “list, description or other grouping of consumers” prepared using such information would be subject to the same restrictions. *See* Proposed § \_\_.3(n)(1)(ii), (SEC version (t)(1)(ii)).

The Agencies may not have contemplated the consequences of such a reading for most financial institutions. A financial institution wishing to distribute customer information for *any* purpose would have to contact each and every one of its customers -- former as well as current, as far back as it maintained customer records -- to provide each customer with appropriate notice and the opportunity to opt out. This would be true even if it only wished to distribute that information pursuant to one of the exceptions to notice and opt-out. For example, a financial institution might wish to use a third-party marketer to solicit new business from customers that had ceased to be the institution’s customers before the Effective Date. If the Privacy Provisions applied to the information, the institution would be unable to distribute the information to its third-party marketer without having provided an appropriate privacy policy notice to its customers, despite the fact that such a distribution falls into an exception. *See* Proposed § \_\_.9(a)(1). In effect, the institution would need to contact all of its former customers directly, in order to get permission to contact them through a third-party marketing firm.

Beyond this initial consequence, such a reading would create significant on-going costs to any financial institution interested in using or disclosing customer information. The institution would have to scrutinize the origin of every piece of information in its possession, looking for

---

<sup>4</sup> The definition of “consumer” does not rule out this reading: a consumer is “an individual who obtains *or has obtained* a financial product or service from you ...”. Proposed § \_\_.3(e)(1) (emphasis added).



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 20

evidence that it had obtained the information either (1) pursuant to this retroactive notice with no consumer opt-out; (2) pursuant to prospective notice with no consumer opt-out; or (3) pursuant to one of the exceptions to the notice and opt-out requirements. It would equally have to scrutinize every piece of information on a customer that it sent to anyone, looking for the same evidence. Even assuming that the institution was able to contact all of its former as well as current customers, this reading of the Proposed Rule would greatly increase every institution's data management costs, and reduce the value of some significant portion of its existing customer database. For those institutions that habitually use, "derive" and share historic data concerning former customers, such as mortgage lenders and servicers, or insurance companies, even larger portions of their business information would be disabled, given the difficulty and/or cost of locating many former customers in order to obtain consent to process their information.

Congress does not appear to have intended to have such an effect. It was well aware that, in inserting the Privacy Provisions, it was imposing federal privacy obligations on businesses for the first time. In order to avoid dislocation caused by this novel obligation, Congress made clear that the Privacy Provisions would not become effective immediately, but only after an appropriate transition period. It also made clear that the Agencies had discretion to write regulations that would carry out the purpose of the Privacy Provisions, even if that meant amplifying or clarifying the effect of the statutory language. *See* Pub. L. 106-102, § 504(a)(1), (b). The purpose of the Privacy Provisions was to regulate, not to prohibit, the distribution of consumer information, and to do so in a way that was consistent in its applicability to all financial institutions. *See id.* §§ 501(a), 504(a)(2). There is no evidence that Congress intended to impose such significant burdens on financial institutions by imposing these privacy obligations. There is certainly no evidence that Congress intended to adversely impact those financial institutions with large databases of customer information on the effective date, or with databases consisting largely of information pertaining to former customers.

In order to avoid the unintended consequences of an unnecessarily restrictive interpretation, we think it important that the Agencies make clear that information provided by or about an individual who is no longer a customer of the institution on the effective date of the Privacy Provisions is not covered by the Privacy Provisions. This clarification might be most appropriate in connection with the so-called "transition rule," Proposed § \_\_.16(b). The transition rule requires a financial institution to provide an initial notice and opportunity to opt out to those persons who are customers of an institution on the effective date. The Agencies could make clear that this limitation means that persons who are no longer customers of an institution on the effective date, or who have been consumers prior to the effective date, are not subject to the Privacy Provisions, and that their nonpublic personal information is likewise not subject to the Privacy Provisions.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 21

*Clarifying the Alternative B definition of “nonpublic personal information” (2): What information is “personally identifiable”?*

The Agencies can also clarify what financial information is “personally identifiable.” *See* Proposed § \_\_.3(o) (NCUA version (p), SEC version (v)). Although the definition is elaborate, including numerous examples and several specific exclusions from the category, it does not address this fundamental question. Logically, the phrase would appear to mean that information directly linked to an identifiable individual is covered by the Privacy Provisions, while information not so linked is not covered. This would be in keeping with the FTC’s interpretation of the Fair Credit Reporting Act, under which information that would otherwise be a consumer report, but which has been “coded ... so that the consumer’s identity is not disclosed” is not a consumer report. 16 C.F.R. § 600.3, Commentary to the Fair Credit Reporting Act, Comment 4-B to Section 603(d). The language of the Proposed Rule, however, does not yet clearly state this. We believe that so long as the information is not identifiable, it should not be protected, and that the Final Rule should make this point unambiguously.

Under the Proposed Rule, “personally identifiable financial information” includes “account balance information, payment history, overdraft history, and credit or debit card purchase information.” Proposed § \_\_.3(o)(2)(i)(B) (NCUA version (p)(2)(i)(B), SEC version (v)(2)(i)(B)). We urge the Agencies to specify that this information, like that identified in the other examples, meets the definition only when it pertains to an identifiable consumer. A mere list of account balances without names or other personal identifiers attached cannot help a third party market to the holders of those accounts or otherwise violate their privacy. The Agencies should therefore make clear that such information is not personally identifiable financial information. Based upon this position, the Agencies should also make clear that a financial institution may collect and disclose information lacking personal identifiers without triggering the requirements of the Proposed Rule.<sup>5</sup> In addition, a third party receiving personally identifiable information may scrub that information of personal identifiers and redisclose it without violating the limits on redisclosure and reuse, and without causing the financial institution that provided it with the information to violate those limits either. *See* Proposed

---

<sup>5</sup> Given the pace of technological change, we think it important that the Agencies provide this clarification in generic terms, rather than by specifying that certain technologies are acceptable. Currently, companies use a variety of anonymous electronic identifiers -- embedded in software, hard-drives, or files attached through web site use such as “cookies” -- to collect depersonalized information in order to provide certain Internet services. In order to encourage this sort of technological diversity, and to permit the Final Rule to grow with technology, we support an exclusion that is defined by the type of information collected (that is, depersonalized information) rather than limited to specific technologies.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 22

§ \_\_.12. If the business disclosing such anonymous information wants, for its own tracking purposes, to “identify” each piece of data by the encrypted name or account number of the consumer, we do not think this information should be considered subject to the Privacy Provisions unless and until it is decrypted.

If the Proposed Rule fails to clarify that disclosing this anonymous information is not subject to the Privacy Provisions, it will jeopardize or encumber many business activities that depend on this information. For example, aggregated financial information, stripped of personal identifiers, constitutes the database from which risk models are constructed and refined. Sometimes, businesses construct their own risk models; other businesses use more general-purpose risk models, such as credit scoring systems or automated underwriting programs. But all of these models are built on the same types of information, and all perform the same function: quantifying risk. These models guide lenders in determining how much interest to charge on individual loans, in order to cover the risks associated with such loans while offering the most competitive rates (that is, the lowest rates consistent with the institution making a profit). Risk models are more effective the more information they have to work with; conversely, the less information is available, the less effective these risk models are at quantifying risk. And when lenders cannot rely upon their risk models, they tend to charge higher rates, in order to avoid losing money to unanticipated or incorrectly quantified risks. Consumers profit from accurate risk models, which are only possible with access to accurate aggregated information.

To take another example, lenders subject to the Community Reinvestment Act, the Fair Housing Act, or other antidiscrimination statutes use statistical modeling to assess their antidiscrimination compliance. Like risk modeling, antidiscrimination modeling is built on aggregated financial information. Also like risk modeling, antidiscrimination modeling is able to do what it does -- detect possibly discriminatory trends -- better and more accurately if it is based on larger amounts of information. Financial institutions that can identify worrisome trends early are better able to correct those trends, thereby fulfilling the purpose of these statutes without the need for expensive, disruptive enforcement actions. Individual consumers and society as a whole profit from more effective antidiscrimination models, which like effective risk models are only possible with access to accurate aggregated information.

Additionally, clamping down on the distribution of aggregated information could disproportionately harm small institutions’ modeling programs. Large institutions, or companies with numerous affiliates, may be able to generate enough data continually to refine their statistical models from their own programs, without resorting to obtaining information from third parties. Smaller institutions, less well-endowed with affiliates, by contrast have no choice but to obtain information from outside their own organizations. If the distribution of aggregated or



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 23

otherwise depersonalized information is curtailed because regulations make it inappropriately subject to the Privacy Provisions, small companies will be disproportionately affected. They will find it difficult to refine their statistical models, and they will find themselves operating with tools that are progressively less and less competitive with those of the larger or better-connected companies.

Unfortunately, regulatory discouragement of the distribution of depersonalized or aggregated information will also deprive these smaller companies of the products that would otherwise restore a competitive balance: off-the-shelf statistical models based on historical data. If an institution can be dissuaded from sharing information that it obtained from its own current customers, to whom it knows it provided privacy policy notices, how much less likely will the institution be to share information obtained from former customers, who may or may not have received such notices? If up-to-date statistical data derived from information obtained with the benefit of privacy disclosures cannot safely be disclosed, who will volunteer to share data, or models “derived using” data, obtained without the benefit of such disclosures? Statistical models cannot be taken apart and cleansed of the effects of data that may not be shared. So regulations that defined “personally identifiable” information either broadly or vaguely would effectively discourage the sale or other distribution of statistical models, or their use by anyone other than their original creators.

Congress specifically intended that the Privacy Provisions not have a disproportionately harsh effect on small institutions, as the Agencies are well aware. *See* H.R. Conf. Rep. 106-434, at 173 (1999), discussed at 65 Fed Reg. 8785. But that is precisely the effect that discouraging distribution of aggregated information would have. Small companies, at a competitive disadvantage because they were deprived of the data necessary to refine their own models, would never be able to catch up by buying models on the open market. A regulatory stance intended to protect consumers would thus hurt them by depriving them of true competitive choice.

By contrast, the risks to consumers from exempting the distribution of aggregated or otherwise depersonalized information from the Privacy Provisions are negligible. So long as the information is truly unable to be traced to individual consumers, those consumers cannot even be contacted, much less experience any loss of privacy from the disclosure. It is true that a person or business who obtains enough depersonalized information, possibly from several sources, may be able to cross-reference that information in such a way as to deduce the identity of individual consumers. If and when that happens, however, the person or business has effectively decoded the information and transformed it into nonpublic personal information, rendering it subject to the Privacy Provisions. As a result, the information is then subject to the reuse and redisclosure provisions of the Proposed Rule, which drastically limit the ability of the decoding person or



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 24

business to use the information. Because the reuse and redisclosure provisions also apply to the business providing the information, foresighted businesses distributing aggregated or otherwise depersonalized information will contractually obligate the recipients of such information not to attempt to deduce the identity of individual consumers. If such a situation then arises, consumers and businesses are protected by the same enforcement mechanisms that protect them with relation to the misdisclosure and misuse of personally identifiable information that has not been depersonalized and repersonalized.

Because of the benefits to consumers, and because of the lack of corresponding risk, we urge the Agencies to permit the free distribution of aggregated or otherwise depersonalized data. Businesses with such information should be able to provide it to businesses that can put it to productive use. So long as this information does not identify and cannot be traced to individual consumers, distribution of this information should not be subject to regulations which were intended to protect consumers against the uncontrolled disclosure of information pertaining directly to them.

*Clarifying the Alternative B definition of “nonpublic personal information” (3): What is a “list, description or other grouping ... derived using personally identifiable financial information”?*

Another way the Agencies could clarify what constitutes nonpublic personal identification would be to define what constitutes a “list, description or other grouping of consumers ... derived using any personally identifiable financial information.” Proposed § \_\_.3(n)(1)(ii) (SEC version (t)(1)(ii)). In its discussion of the applicability of this language, the FTC uses the example of a list of individuals compiled from an institution’s customer lists. 65 Fed. Reg. 11,178. The banking agencies appear to agree that a list compiled from customer lists should be covered by the Privacy Provisions. 65 Fed. Reg. 8774. We agree with the FTC and the banking agencies with respect to this sort of information. A list “derived” from customer lists solely by deleting the fact of the customer relationship is only one small step removed from information defined as nonpublic personal information. If a financial institution distributes a list of individuals and pertinent information about them, the recipient of the list will presume those individuals are the institution’s customers. Such a list should be covered by the Privacy Provisions. But the language of the Proposed Rule could extend to much more than lists of individuals, and much farther than to direct providers of such lists. We urge the Agencies to prevent the ambiguity of this language from swallowing up all sharing of information, however characterized.



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 25

If given their broadest possible meaning, the terms “description” and “grouping” would cause the Privacy Provisions to prohibit a financial institution from describing its own customers in any respect -- with no particular benefit to consumers. If an institution, for example, were to list the top three zip codes of its customers, it would “describe” or “group” consumers (those living in the three zip codes) in a manner derived from nonpublic personal information (the zip codes of its customers). But what harm would this description or grouping cause? The person to whom the institution gave this description or grouping would never be able to learn from it who the institution’s customers were. If this person wanted to market a product or service, he or she would have to market to all persons within the three zip codes. Such marketing would be more narrowly focussed than a nationwide advertising campaign, but there is no suggestion that the Privacy Provisions were intended to limit or discourage geographically targeted marketing. Instead, it was intended to limit the distribution of identifiable information about consumers.

Likewise, the term “derived” could be interpreted so broadly as to prohibit the recipients of coded or otherwise aggregated information from using that information for their own purposes -- again with no particular benefit to consumers. Strictly speaking, any list that an institution prepares on its own behalf, if it does so using even the smallest amount of aggregated information obtained indirectly from another financial institution, is “derived using personally identifiable financial information.” But to take our zip code example, if an institution is given three zip codes and constructs its own marketing list, comprising all of the households in those zip codes, that list does not jeopardize the confidentiality of any nonpublic personal information of the persons on the list. No one can reverse-engineer the list to determine which persons on it are also customers of the financial institution that identified the three zip codes in the first place. The list itself is innocuous from a privacy perspective, and as a result the institution that compiled the list should be able to use it or distribute it, as the institution sees fit, outside the limitations of the Privacy Provisions.

The Agencies should therefore make clear that lists, descriptions and groupings of consumers are only covered by the Privacy Provisions if they permit the recipient of the information to obtain personally identifiable financial information about consumers by “decoding” the list, description or grouping. A statement like “many of our customers live in zip code 20016” should not be covered by the Privacy Provisions, while “every person who lives in zip code 20016 is a customer of ours” should be. The Agencies should specify that generic information is not covered by the Privacy Provisions, so long as it is not specific enough to permit the person receiving the information to “decode” the information and deduce personally identifiable financial information from it.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 26

*Clarifying the Alternative B definition of “nonpublic personal information” (4): What information is “publicly available information”?*

Because nonpublic personal information is defined in part as information that is not “publicly available information,” a final aspect of the definition that the Agencies could clarify concerns the definition of its opposite. The banking agencies’ and the FTC’s versions of Alternative B of the Proposed Rule all define publicly-available information as “any information ... lawfully made available to the general public” from a variety of public sources. Proposed § \_\_.3(p)(1). This makes a large amount of information available for distribution: “information [is] publicly available if it *could be* obtained from one of the public sources listed in the rules, even if was obtained from a source not listed in the definition.” 65 Fed. Reg. 8774, 11,179 (emphasis added). This is clearly superior to the definition in Alternative A, under which information is not publicly available “unless it is obtained from one of the public sources listed in the proposed Rule.” *Id.* But under one reading even Alternative B imposes heavy burdens on a financial institution. Alternative B establishes no safe harbors; as a result, an institution could unwittingly be violating the Privacy Provisions by distributing information that wasn’t actually publicly available, unless it checked first. Alternative B could be read to require an institution to check whether particular pieces of information were in fact available from a public source before disclosing them to a third party as publicly available information. Under this reading, Alternative B (in this respect) would be no less cumbersome than Alternative A. Indeed, because the Proposed Rule does not specify *when* the information must be publicly available (at the time it is obtained? or at the time it is disclosed?), it might prove more cumbersome and provide less certain means of avoiding liability.

By contrast with most of the Agencies’ proposed language, the SEC version provides such certainty and is easier to comply with. The SEC version defines publicly-available information as “any information that you [the financial institution] reasonably believe is lawfully made available to the general public[.]” Proposed § \_\_.3(w)(1), 65 Fed. Reg. 12,372. This definition would make clear that an institution did not need to check the availability of every piece of information prior to disclosing it. Instead, an institution could establish broad guidelines, updated as new information became publicly available, on which to base its information-distribution policies. So long as those guidelines expressed a reasonable belief in what was publicly available, distribution according to those guidelines could be outside the restrictions of the Privacy Provisions.

While easier for businesses to implement, the SEC’s language is no less consumer-friendly than that of the other Agencies. Both would protect from distribution information that is not publicly available: the other Agencies’ version by requiring institutions to check availability

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 27

as a matter of routine, and the SEC's by requiring institutions to establish what they reasonably believe to be publicly available. Both could be enforced by lawsuit: the other Agencies' version by a multitude of individual suits alleging distribution of specific pieces of information that weren't really publicly available, and the SEC's by a smaller number of larger suits challenging institutions' guidelines as unreasonable. In both cases, therefore, consumers would be relatively safe from institutions abusing the definition of publicly-available information in order to evade the restrictions of the Privacy Provisions. The difference is that, with the SEC's version, consumer protection would be purchased at a much lower cost in business compliance efforts. Given its benefits to business and its lack of harm to consumers, the SEC's version of the definition of "nonpublic personal information" should, in our opinion, be adopted by the other Agencies.

*Clarifying the Alternative B definition of "nonpublic personal information" (5): What Internet sites qualify as "widely available media"?*

An additional aspect of the definition of publicly-available information that we are particularly concerned about clarifying deals with the applicability of the term "widely available media" to Internet web sites. See Proposed § \_\_.3(p)(2)(ii), (SEC version (w)(2)(ii)). The example in the Proposed Rule suggests that an Internet website is widely available only if it is "available to the general public without requiring a password or similar restriction." *Id.* Most individuals must pay a fee to an Internet Service Provider ("ISP") for the convenience of accessing the Internet from their homes. In and of itself, such a fee could be interpreted to be a "similar restriction," casting doubt on whether an individual in such a situation was obtaining publicly-available information through a widely-available medium. To make the formulation of the Proposed Rule still more problematic, some ISP fees may give the individual access to information proprietary to the ISP and available only to its subscribers -- in which case the fee really would be such a restriction. The Agencies' formulation provides no guidance about what on the Internet is truly publicly-available information.

It appears that the Agencies were trying to capture the concept of free information -- which as we have pointed out is the revolutionary aspect of the Internet, and which therefore deserves to be singled out in the final Rule. We urge the Agencies to make clear that widely-available media include Internet sites that an institution reasonably believes an individual could access from a publicly-available facility such as a computer in a public library, without that individual having to provide a password or pay a fee.



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 28

*Who is an "affiliate"?*

A final definition that should be clarified -- that of who is an "affiliate" of a financial institution -- could also be made uniform along lines suggested by the SEC. All versions of the Proposed Rule define an affiliate as "any company that controls, is controlled by, or is under common control with" a regulated company. Proposed § \_\_.3(a). The Agencies differ in their definitions of "control," however, with the SEC's definition being significantly clearer and therefore easier to work with.

Most versions of the Proposed Rule (those of the banking agencies, the NCUA and the FTC) define "control" in three ways, of which only one has an objective component:

Control of a company means:

- (1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
- (2) Control in any manner over the election of a majority of the directors, trustees or general partners ... of the company; or
- (3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

Proposed § \_\_.3(g). As these agencies note, this definition is the same as that found in Section 23A of the Federal Reserve Act. 65 Fed. Reg. 8772, 10,990, 11,176. But the Federal Reserve Act definition is not a model of clarity, and over the years the Board has had to issue a series of interpretive letters explaining the meaning of these provisions. Even if the Agencies were to adopt the Board's interpretations along with this definition of control, knowing who was an affiliate for purposes of the Privacy Provisions would be a matter of significant uncertainty. Because distributing information to actual affiliates is not subject to the Privacy Provisions, but distributing information to apparent affiliates *is*, companies need to know with certainty who their affiliates are. Any significant uncertainty undermines the ability of companies to take advantage comfortably of the whole exception for distributing information to affiliates, and thereby runs counter to the Congressional intent to leave information-sharing among affiliates untouched by the Privacy Provisions. *See, e.g.,* Pub. L. 106-102 § 502(a). As with other sources of regulatory uncertainty, it only has the effect of creating uneven compliance, with companies worried about potential liability taking very conservative positions, and companies not worried about potential liability taking very aggressive positions about who their affiliates are.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 29

The SEC's version of the definition of "control" shows how avoidable this is. The Proposed SEC Regulation, while not rigid, nevertheless establishes clear presumptions about who is or is not in control of whom:

Control means the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. Any person who owns beneficially, either directly or through one or more controlled companies, more than 25 percent of the voting securities of any company is presumed to control the company. Any person who does not own 25 percent of the voting securities of a company will be presumed not to control the company. Any presumption regarding control may be rebutted by evidence ...

65 Fed. Reg. 12,370-71 (Proposed § \_\_.3(i)). The SEC's language allows regulators the flexibility to take action in situations that violate the spirit, though not the letter, of the regulations. Nevertheless, its clear presumption that 25% ownership of voting securities is the significant threshold allows companies to plan on the basis of reasonably firm knowledge of who their affiliates are and are not. Because the SEC's definition is probably somewhat narrower than that of the other Agencies, its effect will probably be to bring more forms of information-sharing within the scope of the Privacy Provisions -- a consumer-friendly effect whose cost to business is more than compensated for by the lower compliance costs of using the SEC's definition. We urge the other Agencies to adopt it.

**Notice, Opt-Out, Distribution and Reuse Requirements Need to Include Guidance Specifically Applicable to the Internet Context**

While clarifying key definitions is important for financial institutions that do business with consumers over the Internet, we believe that the Agencies must take other actions as well in order to make the Proposed Rule Internet-friendly. Specifically, they must provide guidance concerning compliance with the notice, opt-out, distribution and reuse provisions of the Proposed Rule that make these requirements meaningful under the special circumstances of the Internet.

The Act provides that "a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, of such institution's policies and practices...". PL 106-102, § 503(a). Congress did not establish any more stringent standard for delivery of privacy policy disclosures "on-line" than in an "off-line" context, but it appears that the Agencies have

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 30

inadvertently established a higher bar for doing business on line than for doing business off-line. Guidance on the following issues could restore the balance Congress intended.

*Actual Notice*

The Proposed Rule provides two examples concerning the requirement that a consumer receive “actual notice” of a business’s privacy policies and practices. A business can reasonably expect a consumer to receive actual notice if the business “post[s] the notice on the electronic site and require[s] the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service[.]” Proposed § \_\_.4(d)(5)(i)(C). A business cannot have such an expectation if it “send[s] the notice via electronic mail to a consumer who obtains a financial product or service with you in person or through the mail and who does not agree to receive the notice electronically.” Proposed § \_\_.4(d)(5)(ii)(B). The Agencies may believe that these two examples establish a rule concerning what constitutes effective electronic notice that is both predictable and even-handed in its treatment of electronic and paper disclosures. In fact, the two examples leave several significant problems unaddressed:

- May a business provide the privacy policy by e-mail to a consumer who consents to such delivery? We think it should be permitted to do so, and we think the second of the examples noted above implies this by negative inference. An institution should not be required to give electronic notice exclusively using a pop-up screen that requires response before proceeding, which would effectively require acceptance before proceeding. Limiting electronic disclosure to such a narrow technological solution would mean that the electronic opt-out was an opt-in for all practical purposes. But Congress considered and specifically rejected an amendment to the Act that would have required businesses to offer consumers an opt-in. If a business wants to use opt-ins, for customer relation purposes or to establish consumer consent to sharing, then it should be able to. But such an opt-in should not be mandated for electronic disclosures, given that it is not required for paper disclosures. We would like confirmation, in the form of a specific example or regulatory language, that any mode of delivery specifically agreed to by the consumer is permissible.
- Must a business provide a separate notice for each site? We think there should be no limitation on the range of Internet addresses or sub-addresses covered by any particular privacy policy disclosure, so long as it is clear to the consumer which addresses or sub-addresses the disclosure does cover. But currently, the only guidance the Proposed Rule provides refers to a notice on a single “site,” without defining what constitutes a site. The Agencies need to make clear that a privacy policy disclosure can apply as broadly or as



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 31

narrowly as a business wishes it to (subject to the requirement that the limits of applicability of the notice be clear), in order to avoid tying the Proposed Rule to the current technological standard for what constitutes a “site.”

- Must a business post a separate notice for each instance in which it provides a financial product or service over the Internet? Again, we think there should be no limitation on the range of products or services to which any particular privacy policy disclosure applies. If a business wishes, it should be able to use a single privacy policy disclosure with reference to as many or as few products or services as it wishes, again subject to the requirement that the limits of applicability of the notice should be clear. Using appropriate tracking technology, it may be possible to provide a small number of comprehensive privacy policy disclosures, rather than bombarding a consumer with redundant requests that he or she read and acknowledge privacy policy disclosures each time he or she accesses a web site to request a financial product or service. This increase in efficiency would cause no diminution in the consumer’s privacy protection. We urge the Agencies to make clear that companies can, if they wish, provide such comprehensive disclosures.
- Must a business post the notice on its own site, or may it link to a third party service provider’s site? The Proposed Rule appears to specify that the business post the privacy policy notice on its own “site.” We see no reason, however, why a business should not be able to create a non-discretionary link to a third party’s site where the privacy policy notice is posted, so long as the effect is the same as a posting on the business’s own site, and so long as the legal responsibility for the posting lies with the business rather than its third-party service provider.

Although the Proposed Rule may leave unanswered other Internet-related questions about actual notice, we think these are the most important, and we urge the Agencies to clarify their position on all of these. The flexibility of Internet technology, its ability to parcel out responsibilities among numerous parties, and its ability to provide linkages among diverse product and service providers are all aspects that provide significant benefits to consumers. The Agencies should not permit these same aspects to confer contingent legal liability on Internet financial services businesses through lack of regulatory clarity.

*Co-Branded Products and Services*

In the same way, it would benefit providers of financial services over the Internet if the Agencies were to clarify how to comply with the Privacy Provisions in a situation, common on



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 32

the Internet, where a financial product or service is provided through a co-branded web site. The Proposed Rule does not discuss co-branding at all. However, it appears to contemplate a rough parity whereby the provision of one financial product by one business produces the need for one privacy policy notice. Under such a logic, it would appear that a product or service provided through a co-branded site, if truly provided by both of the co-branded entities and not by one as the agent of the other, would require two notices.

We do not think this solution is consumer-friendly, and we think instead that it should be possible for the co-branded businesses to provide a single privacy policy notice applicable to both businesses. We have noted above that we see no harm in permitting businesses to provide blanket notices that cover more than one product or service, so long as those notices are clear about what they cover. By the same token, there would appear to be no harm to consumers if two businesses provided a joint disclosure, so long as that notice clearly and accurately described both institutions' policies. Such joint disclosure would be more convenient and comprehensible to the consumer than receiving a series of (possibly contradictory) disclosures from individual participants in the co-branded site. Based upon its benefits and its lack of harm, joint disclosure in such circumstances should explicitly be permitted.

*Joint Accounts*

Another area that we think it important for the Agencies to clarify concerns delivery of privacy policy notices to persons setting up or holding joint accounts. The Proposed Rule does not specifically discuss how the notice and opt-out requirements apply to joint accounts, and both the banking agencies and the FTC have requested comments on the issue. 65 Fed. Reg. 8778, 11,182. We think that any specification of requirements for joint accounts must take into account the reality that most "joint" applications involve one person doing a disproportionate share of the applicants' work. This is clearly the case in the Internet context: a joint application is submitted from a single computer with a single keyboard. The notice and opt-out requirements should reflect this reality, permitting a financial institution to provide a single notice and a single opt-out for a joint account, covering all information provided in connection with that account. The financial institution should be able to provide that notice and opt-out to any joint account holder, leaving it to that person to consult with the other joint account holders about whether to opt out. And any one of the joint account holders should be able to exercise the opt-out, restricting distribution of the information associated with the account. In such case, the Agencies would recognize by rule the legitimacy of a presumption that a communication from any joint account holder was a communication on behalf of all.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 33

The alternative, requiring that every joint account holder receive a notice and opt-out, would be unworkable for businesses and unfriendly to consumers. Providing multiple disclosures would be cumbersome even with paper applications. Financial institutions would have to keep track of whether all, or only some, of the joint account holders had opted out. And if joint account holders disagreed about opting out, or if one was more prompt than the others in returning the opt-out form, financial institutions would be in the impossible position of having to winnow information from the joint account, restricting the distribution of information personal to one, but not all account holders. The procedure would be even more difficult with electronic applications, given the need to designate specific computers as being under the control of specific persons for purposes of sending notices and receiving acknowledgments or opt-outs. And the only effect all this complication would have on consumers would be to draw out the period of uncertainty during which a consumer could not know whether all the information pertaining to an account was or was not restricted by opt-out. We see no benefit to providing such a cumbersome solution, and we urge the Agencies instead to make clear that only one notice need be sent for a joint account.

*Maximize the Efficiencies Created by Electronic Delivery of Notices*

We applaud the Agencies' willingness to permit privacy policy notices to be delivered electronically with the consent of consumers. We think that electronic delivery will quickly become the most popular method for consumers to obtain privacy information and for businesses to comply with the Privacy Provisions. It will become clear, if it is not already, that duplication of electronic delivery of notices with delivery of paper copies, as has been proposed by some, is entirely unnecessary -- a position that we strongly adhere to, and which we think the Agencies should clearly endorse in the Proposed Rule. Nevertheless, we understand the concern of consumer advocates that the electronic delivery of privacy policy notices be certain. For this reason, we think that the Agencies should make clear that financial institutions may, and indeed are encouraged to, track the electronic delivery of privacy policy notices by electronic methods, with notice to consumers but without opt-out by consumers. Regulatory support for the use of such technology will permit the Internet financial services industry to meet consumer privacy expectations without sacrificing the efficiencies of electronic commerce.

In addition, the Agencies can enhance the efficiency of such electronic delivery by permitting financial institutions to accept electronic opt-outs only through designated means. The FTC has solicited comments on whether financial institutions should be required to accept opt-outs "through any means the institution has already established to communicate with consumers." 65 Fed. Reg. 11,183. Such a requirement would eliminate the efficiency benefits and lower consumer costs associated with the electronic delivery of notices and electronic receipt

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 34

of opt-outs. An Internet-based institution would have to accept nonelectronic opt-outs at any postal address it advertised, and oral opt-outs (if permitted by the final Rule) at any telephone number it advertised. If an institution maintained multiple web sites, it would have to reconfigure those web sites to accept the exercise of the opt-out right. Making these provisions would add expense without providing additional consumer benefit: given that consumers must consent to the receipt of electronic disclosures, they will only consent to a disclosure system that is already convenient to them; they will not care about receiving additional undisclosed conveniences that they never intended to use. With regard to electronic disclosures, at least, the Agencies should make clear that institutions can designate the exclusive electronic means whereby consumers can exercise the opt-out right. Making this change will help to lock in the benefits to consumers of permitting the electronic delivery of privacy policy notices and the electronic acceptance of opt-outs.

*Establish Electronic “Reasonable Opportunity” Standards for Opt-Outs*

The Proposed Rule should also clarify the issue of what, in the context of the Internet, constitutes a “reasonable opportunity” for a consumer to opt out. The Proposed Rule provides two examples of a reasonable opportunity. With a customer, a financial institution may

mail the notices required in ... this section to the consumer and allow the consumer a reasonable period of time, such as 30 days, to opt out.

Proposed § \_\_.7(a)(3)(i). In addition, in an isolated transaction, a financial institution may

provide the consumer with the required notices at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

Proposed § \_\_.7(a)(3)(ii). The banking agencies and the FTC have solicited comments on whether an additional example “in the context of transactions conducted using an electronic medium would be helpful.” 65 Fed. Reg. 8778, 11,182. We think that an additional example would be helpful, given that the two examples in the Proposed Rule leave so many possible consumer relationships unaddressed.

Specifically, the Agencies should provide clear guidance that applies to situations in which a financial institution provides electronic notices to its customer, and in which a financial institution provides electronic notice to a consumer in connection with something more than an isolated transaction. The reasonableness of the response period for electronic notices should not



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 35

be measured by the slower pace required in connection with notices being mailed. Electronic delivery is a reliable delivery mechanism, and delivery failures are easy to detect and correct, so there is no reason to require a financial institution to wait thirty days to permit a consumer or customer to respond to an electronic notice. At the same time, because the privacy policy notice may be a complex document, it may not always be appropriate to require the consumer or customer to read, acknowledge and consent immediately as a condition to proceeding with the transaction. We therefore urge the Agencies to insert at least one additional example, establishing that what constitutes a reasonable opportunity in the electronic context is some period significantly less than thirty days, though longer than that given to a consumer in an isolated transaction. We think three (3) days is a period appropriate for both consumers and customers. The federally mandated cooling-off period for certain persons borrowing on the security of their principal dwellings is currently three days. 15 U.S.C. § 1635(a). If three days is reasonable time to decide about such a significant issue, it should be reasonable time for the consumer or customer to make the decision whether to permit nonpublic personal information about himself or herself to be distributed.

*Permit Businesses to Take Maximum Advantage of Non-Marketing Outsourcing Opportunities*

The Proposed Rule should also reflect the reality that businesses outsource many non-marketing functions to third party service providers. Moreover, businesses regularly change such third party service providers to obtain better quality services at more favorable prices, which in turn enables businesses to offer their products and services to consumers in a more efficient and cost-effective manner. This is especially true for companies that operate in a flexible business environment, such as over the Internet.

The Proposed Rule should not require a business to provide the change-in-terms notice to consumers mandated under Proposed § \_\_.8 each time that a change in its outsourcing arrangements for non-marketing functions might result in a new category of third party service provider utilized. Such a requirement would impose a substantial, additional economic cost on businesses, especially new businesses. Indeed, the burden of redisclosure would fall disproportionately on smaller businesses, which have a greater need to outsource functions, are more likely to change third-party service providers and are the least able to bear the economic costs of continual redisclosure. Such a regulatory cost could inhibit the ability of businesses to change to more efficient third party service providers when economically appropriate. It would be unfortunate and unnecessarily wasteful if the Proposed Rule had the effect of freezing existing business relationships and entrenching existing inefficiencies, rather than permitting businesses to seek out new opportunities as they arose.

Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 36

Rather than requiring a business to provide a change-in-terms notice every time that it changes an outsourced non-marketing service provider, we think this type of routine change with respect to non-marketing functions should be included as an exception to the notice and opt-out requirements in either Proposed § \_\_.10 or Proposed § \_\_.11. If the Agencies conclude that such changes in outsourcing arrangements should not be excluded from the notice and opt-out requirements per se, then, at a minimum, changes in the identity of third party service providers that do not affect the categories of information disclosed should be clearly exempted from the change-in-terms notice requirement.

*Establish Reasonableness Standard for Consumer Consent*

An additional area where greater clarity could result in more efficient and more consumer-friendly delivery of financial services has to do with obtaining consumer consent to information-sharing. The Proposed Rule permits a financial institution to distribute information “with the consent or at the direction of the consumer” without the need to provide notice or opt-out. Proposed § \_\_.11(a)(1). The Agencies have invited comments on whether specific safeguards should be added in order to minimize the potential for consumer confusion. 65 Fed. Reg. 8780, 10,197, 11,184, 12,362. Because we think that securing informed consumer consent can be an exceptionally effective method of streamlining the sharing of information, particularly over the Internet, we are eager to take up the Agencies’ invitation. We believe the Agencies should establish a reasonableness standard for informed consumer consent. Consent should be effective if a reasonable person in the consumer’s position would have been aware of the nature of the information the institution would be sharing pursuant to the consent, and of the persons with whom the institution would be sharing the information. If the institution wishes to obtain the consumer’s consent to specific forms of information-sharing, or to blanket distribution of the consumer’s information, that choice should be up to the institution. So long as its communication to the consumer would clearly disclose to a reasonable person what the consent would entail, an consent secured pursuant to that communication should be honored.

*Give Institutions Flexibility in the Distribution and Use of Information They Receive*

An additional way the Agencies could assist Internet-based institutions in providing financial services efficiently to consumers would be to make the exceptions to the notice and opt-out provisions, Proposed § \_\_.9, \_\_.10 and \_\_.11 (each an “Exception,” collectively the “Exceptions”) fully available to companies that redistribute and reuse information. With regard to redistribution, the Proposed Rule prohibits a company receiving information from a nonaffiliated financial institution from disclosing that information to another nonaffiliated party “unless the disclosure would be lawful if the financial institution made it directly to such other



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 37

person.” Proposed § \_\_.12(a)(1). The Agencies describe this rule as placing the receiving company in the “shoes of the institution that disclosed the information” and suggest that it permits the receiving institution to use that information pursuant to any of the Exceptions. 65 Fed. Reg. 8780, 10,997, 11,184, 12,364. But without explicit guidance in the regulatory language itself, the shoes-of-the-original-institution rule could be interpreted far more narrowly, leading to unintended results:

- Company A receives nonpublic personal information from Company B in the course of providing back-office settlement services for Company B, pursuant to the Exception at Proposed § \_\_.9. Subsequently, Company A may wish to disclose some of this information to expert witnesses in the course of defending an unrelated claim against it. This would appear to be permitted by Proposed § \_\_.11(a)(2)(ii), under which information may be disclosed “to protect against ... claims or other liability[.]” But it could be argued that, because Company B is not being sued, Company B would not be able to disclose this information pursuant to this Exception to its expert witnesses, and therefore Company A cannot disclose the information to its own expert witnesses either.

Similar problems arise with the re-use provisions of the Proposed Rule. The Proposed Rule prohibits an institution, receiving nonpublic personal information pursuant to the Exceptions, from using that information except “for the purpose of that exception.” Proposed § \_\_.12(a)(2), (b)(2). Under a strict reading of this language, a business could find itself stripped of legal protection because of its inability to use information that it had received appropriately:

- Company A, which performs post-closing transactional services, might receive information from Company B under the exception for distribution of information “as necessary to effect, administer or enforce a transaction ... authorized by the consumer[.]” Proposed § \_\_.10(a)(1). If prohibited from using that information for any other of the Exceptions, Company A would therefore be unable to use that information “to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability.” Proposed § \_\_.11(a)(2)(iii).

Given that the Exceptions permit institutions to conduct necessary business activities that are noncontroversial for privacy purposes in an efficient manner, any limitation on the effectiveness of the Exceptions increases the cost of complying with, and the inefficiencies created by, the Privacy Provisions. The Agencies should therefore be careful not to disable the Exceptions through excessive limitations that do not protect consumers. The Exceptions exist because the Agencies, following Congress, determined these forms of information-sharing, and use pursuant to such information-sharing, to be noncontroversial for privacy purposes. *See* Pub. L. 106-102, §

502(b)(2), (e). If use pursuant to one of the Exceptions is noncontroversial, so should use pursuant to any of the Exceptions. Consumers are not given additional protections by limiting businesses' ability to use the Exceptions -- they are only given additional costs, passed on by businesses unable to operate as efficiently as they would like to be able to.

For these reasons, we think that the Final Rule should provide clear redisclosure and reuse rules that permit the reasonable use of any applicable Exceptions by recipients of nonpublic personal information. A business that receives information from a financial institution should be able to disclose that information to third parties if the original institution could have disclosed the information to the same third parties, or if the business can do so consistent with one of the Exceptions. A business that receives information from a financial institution pursuant to any Exception should be able to use that information pursuant to any applicable Exception.

### **Guidance as to Legal Responsibilities**

Once they have clarified the definitions crucial to determining compliance, as well as the requirements for providing electronic notice and opt-out, the Agencies can complete the job of making compliance with the Privacy Provisions in the Internet context possible by answering some of the questions about legal responsibilities left open by the Proposed Rule.

#### *Responsibility for Third Party Use of Information*

A financial institution disclosing information to nonaffiliated third parties that perform services for the institution or function on its behalf must contractually require such third parties to maintain the confidentiality of the information and limit the third parties' use of the information. Proposed § \_\_.9(a)(2). If a financial institution enters into such a contract, and the third party violates these limitations, it is clear that the third party is in breach of the contract. In addition, the third party is probably in breach of the Proposed Rule, given the limitations on redisclosure and reuse of information. *See* Proposed § \_\_.12(b)(2). Both of these outcomes make sense. But we are concerned that, without clarification from the Agencies, the financial institution itself will be held in violation as well, despite the fact that it is blameless. Given the strong effect that the threat of even ill-founded litigation has on the growth of new industries such as those developing in the Internet environment, we urge the Agencies to make clear that, in the situation outlined above, the financial institution is not liable under the Privacy Provisions for the breach of the confidentiality agreement by its third-party service provider.



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 39

*Effects of Overlapping Federal Requirements and Permissions*

The Privacy Provisions cover subject matter that has been largely unregulated up to now by the federal government, but a few existing laws and regulations already cover aspects of information-sharing. The Agencies recognize this fact but do not appear to think they can provide guidance as to the interaction of the Privacy Provisions with these existing laws and regulations 65 Fed. Reg. 8774, 10,992, 11,179. We think that the Agencies not only can, but should, provide such guidance if appropriate. One example where such guidance would be welcome concerns the interaction of the Privacy Provisions with the Fair Credit Reporting Act (“FCRA”), 12 U.S.C. §§ 1681 *et seq.* The Privacy Provisions expressly cannot “modify, limit or supersede” FCRA, except in minor respects, and cannot establish any presumption as to what constitutes “transaction or experience” information for affiliate information-sharing purposes under FCRA. Pub. L. 106-102, Sec. 506(c). But the Agencies can still interpret the Privacy Provisions as comporting with FCRA, or not doing so, in a variety of ways. For example, it would not be unreasonable to conclude that disclosures of information “necessary to effect, administer or enforce a transaction requested or authorized by the consumer” under Proposed § \_\_.10(a)(1) *per se* include all disclosures that, if made by a consumer reporting agency, would be pursuant to a permissible purpose under 12 U.S.C. § 1681b(a). If the Agencies can reach this conclusion, they should state this explicitly. Although the two statutes are distinct, we would urge the Agencies to consider how much it is possible to craft rules for the Act that are consistent with the known rules of the FCRA.

We also urge the Agencies to consider explicitly the interaction of the Act with other federal rules. For example, it seems appropriate that they answer the question of whether Internal Revenue Service rules governing the use of tax return information preempt inconsistent aspects of the Proposed Rule (and if so, what those aspects are). They should also explicitly address the issue of extraterritoriality, consistent with the Board’s regulatory treatment of consumer-protection statutes under its jurisdiction, as well as with the long-standing rule of statutory interpretation that laws are not given extraterritorial effect unless specifically intended to by Congress. The Agencies should state, for example, that a transaction booked at a financial institution’s branch outside the United States is not covered by the regulation. Any such explicit limitation should be consistent with any potential “safe harbor” for U.S. companies established with respect to the EU Directive on Data Protection.



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 40

*Postpone Mandatory Compliance with the Privacy Provisions*

Legal responsibilities will begin to attach to financial institutions as soon as the Privacy Provisions become effective. For new consumers and customers, the Proposed Rule establishes an effective date of November 13, 2000, while for existing customers as of that date the financial institution has thirty days in which to provide and process notices and opt-outs. Proposed § \_\_.16. Given how many businesses still do not realize that they may be construed to be financial institutions covered under the Privacy Provisions, we think it will be extremely difficult to produce widespread compliance with these complicated provisions in such a short period.

Compliance by businesses that know they are covered by the Privacy Provisions will be difficult enough. Financial institutions with large customer bases will find it difficult to contact all of their existing customers and processing their opt-out requests by December 13, 2000, especially given that they will not know until at best May 13 what form the notice and opt-out will need to take. Perhaps more difficult, electronic financial service providers are already writing software for products that will be delivered in the year 2001. They should not be forced to choose between delaying product development for several months in order to take into account the requirements of the Privacy Provisions, or preparing products that they cannot be sure will be in compliance with the law when sold. Too-quick implementation will increase compliance costs and/or cause inadvertent noncompliance.

Rather than permitting the Privacy Provisions to appear ineffectual, we urge the Agencies to postpone the effective date of the Privacy Provisions. The Board, mandating a similarly dramatic regulatory transition after passage of the Truth In Lending Simplification Act in 1980, created a one-year voluntary compliance period, followed by full effectiveness for the redrafted Regulation Z. See Board, Official Staff Commentary to Regulation Z, Introduction-(7). Following this precedent, the Agencies could make compliance with the Final Rule voluntary from November 13, 2000 to November 12, 2001, and mandatory on November 13, 2001.

**Conclusion**

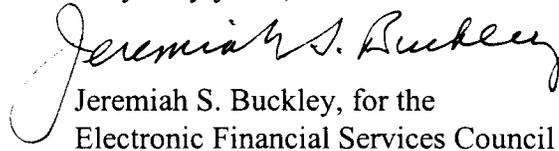
Given the compressed schedule under which the Agencies operated, the Proposed Rule represents an excellent first step toward providing guidance for businesses seeking to comply



Comment on Proposed Rule  
Gramm-Leach-Bliley Act Privacy Provisions  
Page 41

with the Privacy Provisions. However, for the reasons stated above and in our letter to the Board dated March 6, 2000, we believe that, to be effective both as a notice of rulemaking and as the basis for a Final Rule, the Proposed Rule needs to be redrafted to define more clearly what businesses are "financial institutions" falling within the scope of the Privacy Provisions. In addition, we hope that the Final Rule will provide clearer guidance regarding the applicability of the Privacy Provisions to the delivery of financial products or services over the Internet, particularly in the areas we have identified above. We hope that our comments will be of help in making the Final Rule useful to electronic financial service providers and beneficial to consumers obtaining financial products and services electronically.

Very truly yours,

  
Jeremiah S. Buckley, for the  
Electronic Financial Services Council

Attachment  
DOCSW\35640.12

**Electronic  
Financial  
Services  
Council**



1717  
Pennsylvania  
Avenue, N.W.,  
Suite 500  
Washington,  
D.C. 20006

202-974-1000

info@efscouncil.org

March 6, 2000

---

*Via Hand Delivery*

The Board of Governors of the Federal Reserve System  
20th and C Streets, N.W.  
Washington, D.C. 20551  
Attn.: Jennifer J. Johnson, Secretary

RE: Docket No. 5-1058, Gramm-Leach-Bliley Act Privacy Regulations  
Request for Clarification of Terms

Dear Governors:

The Electronic Financial Services Council, which represents companies that deliver financial services over the Internet, is seeking to comment on the proposed regulations implementing the privacy provisions of the Gramm-Leach-Bliley Act (the "Act"), Pub. L. 106-102, Title V, Subtitle A. As you know, federal financial regulators, including the Board of Governors of the Federal Reserve System ("Federal Reserve"), and the Federal Trade Commission ("FTC") have in recent weeks issued proposed regulations implementing the Act.

It is important for providers of financial services to establish clear, effective and legally compliant privacy protections for consumers. However, companies which will be subject to the proposed regulations are severely handicapped in understanding or commenting on the agencies' proposals so long as it is not clear to whom the proposed regulations will apply. Many businesses that would want to comment on privacy issues affecting them do not realize that these proposed regulations are in fact intended to apply to them. In order for the notice and comment process on the proposed regulations to be meaningful, we believe that the Federal Reserve should more clearly and specifically articulate the meaning of the terms that define the applicability of the regulations -- "financial institution" and "financial product or service" -- before the close of the comment period.

*Uncertainty Caused by Vague and Ambiguous Definitions*

The proposed regulations apply to "financial institutions" offering "financial products or services." The proposed regulations define a financial institution as "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k))." Proposed 12 C.F.R. 216.3(j)(1). The proposed regulations define a financial product

or service as "any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k))." Proposed 12 C.F.R. 216.3(k)(1).<sup>1</sup> The cited Section 4(k) of the Bank Holding Company Act, however, merely permits a financial holding company to engage in any activity that:

the [Federal Reserve] Board determines ... (by regulation or order) (A) to be financial in nature or incidental to such financial activity; or (B) is complementary to a financial activity and does not pose a substantial risk to the safety or soundness of depository institutions or the financial system generally[.]

12 U.S.C. 1843k(k)(1). Section 4(k) does, it is true, specify certain activities that are "financial in nature." See 12 U.S.C. 1843k(k)(4). These "specified" activities, however, include:

any activity that the Board has determined, by order or regulation that is in effect on the date of the enactment of the Gramm-Leach-Bliley Act, to be so closely related to banking or managing or controlling banks as to be a proper incident thereto (subject to the same terms and conditions contained in such order or regulation, unless modified by the Board).

12 U.S.C. 1843k(k)(4)(F). The scope of the proposed regulations therefore depends not only upon the reach of a category that has yet to be defined, but also upon a series of prior Federal Reserve determinations which have not yet been brought together in one place for the purpose of notifying parties who may be affected by the regulations. As a result, the proposed regulations' simple reference to section 4(k) of the Bank Holding Company Act fails to provide notice to potentially affected parties. Its main effect is to suggest that more things are financial products or services, more institutions are financial institutions, and the proposed regulations apply more broadly than one would expect.

### *Potential Scope of the Ambiguity*

An example might help to show the potential scope of this ambiguity. Among the activities the Federal Reserve has determined to be "so closely related to banking or managing or controlling banks as to be a proper incident thereto" is:

---

<sup>1</sup> We note that proposed regulations issued by the Federal Trade Commission are identical, with the exception that they do not include the words "or incidental to such financial activities" and "incidental to such a financial activity" in the corresponding definitions. Proposed § 313.3(j)(1), (k)(1).

Providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if—

(A) the data to be processed or furnished are financial, banking, or economic; and

(B) The hardware provided in connection therewith is offered only in conjunction with software designed and marketed for the processing and transmission of financial, banking, or economic data, and where the general purpose hardware does not constitute more than 30 percent of the cost of any packaged offering.

12 C.F.R. 225.28(a), (b)(14). Does this mean that a software vendor, or an Internet portal, would be considered a financial institution for purposes of the Act?<sup>2</sup> We believe that very few companies undertaking these activities are aware that they may be subject to the proposed regulations. The agencies will therefore not have the benefit of these companies' comments on the proposed regulations.

When it enacted the Administrative Procedures Act ("APA"), 5 U.S.C. 551 *et. seq.*, Congress emphasized the importance of providing notice to all parties affected by a proposed regulation, in order to obtain meaningful comments, and to allow such parties to express their legitimate interests and concerns:

Agency notice must be sufficient to fairly apprise interested parties of the issues involved, so that they may present responsive data or argument relating thereto.

---

<sup>2</sup> We note that the Office of the Comptroller of the Currency ("OCC") has already determined that a number of activities not generally associated with financial services may be "part of or incidental to the business of banking," including hosting commercial web sites, registering merchants with search engines, obtaining URLs, providing electronic communications pathways for product ordering and payment, providing merchants with software that will enable them to design their websites, providing links to third party vendors' websites, and building web sites for merchants as part of an Internet merchant hosting service package. OCC Interpretive Letter No. 875 (October 31, 1999); OCC Interpretive Letter No. 856 (March 6, 1999); OCC Conditional Approval No. 304 (March 5, 1999); OCC Corporate Decision No. 97-60 (July 1, 1997). While these rulings are not binding on the Federal Reserve, they suggest how broadly a reasonable person might think the Federal Reserve could interpret its own regulations.

Sen. Doc. No. 248, 79th Cong. 2d Sess. 200 (1946). A more explicit definition of the scope of the proposed regulations would be more consistent with the intent of Congress in passing the APA.

*Guidance Needed from the Federal Reserve*

It would appear that, among the agencies proposing privacy regulations, the Federal Reserve is the appropriate agency to provide specificity regarding what businesses will be affected by the regulations. While a number of federal agencies must propose privacy regulations, only the Federal Reserve can define what constitutes an activity "financial in nature," and thereby define the scope of those privacy regulations. We believe that, in order to comply with the spirit of the APA and the "plain language" provision in Section 722 of the Gramm-Leach-Bliley Act, the Federal Reserve must provide a clearer definition of the entities subject to the proposed regulations before permitting the comment period on those proposed regulations to close.

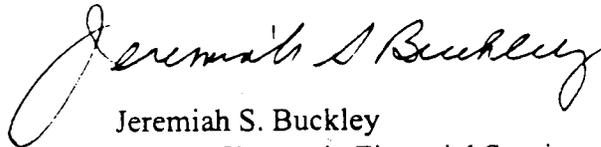
Companies that, unbeknownst to themselves, have become subject to privacy regulations about which they had no notice and no opportunity to comment may be unable to comply. Even companies which are aware that aspects of their activities may be subject to the proposed regulations, will be severely handicapped in commenting on or complying with the regulations unless they have a more specific statement of which aspects of their activities are contemplated to fall within the scope of the regulations' requirements. As you can appreciate, leaving such matters to speculation makes meaningful comment almost impossible.

Members of the Electronic Financial Services Council strongly support implementation of effective privacy regulations. Our members are universally committed to protecting the privacy of consumer financial information. But we believe that the most effective method of protecting consumer privacy, and the method intended by Congress in passing the Gramm-Leach-Bliley Act, is to identify clearly what new obligations apply and the businesses to which those obligations apply. At a minimum, the Federal Reserve can provide specific guidance as to what constitutes an activity permitted for a bank holding company prior to the enactment of the Act. It could also provide clear standards for determining what new activities will be permitted under the Act as activities "financial in nature." If it is unclear whether a category of activities is or is not covered, the Federal Reserve and the other agencies proposing regulations may wish to specifically exclude such categories of activity from the scope of the Act until clear guidance can be provided. This would help to establish what institutions are "financial institutions," what products and services are "financial products and services," and therefore what companies are covered by the proposed privacy regulations. If the Board deems it appropriate, we would

Board of Governors of the Federal Reserve System  
March 6, 2000  
Page 5

appreciate the opportunity to have an on-the-record meeting with your staff to discuss ways in which the issues in this letter can be addressed.

Yours sincerely,



Jeremiah S. Buckley  
For the Electronic Financial Services Council

cc: Virgil Mattingly, Esq.  
Oliver Ireland, Esq.  
Office of the Comptroller of the Currency, Julie Williams, Esq. and Amy Friend, Esq.  
Office of Thrift Supervision, Christine Harrington, Esq.  
Federal Deposit Insurance Corporation, Mr. Robert E. Feldman  
Federal Trade Commission, Kellie A. Cosgrove, Esq. and Clarke Brinckerhoff, Esq.  
Securities and Exchange Commission, Harvey Goldschmid, Esq.  
National Credit Union Administration, Robert M. Fenner, Esq.

DOCSW\35661.5