

**Before the
Federal Trade Commission
Washington, D.C.**

**Gramm-Leach-Bliley Act Privacy Rule
16 CFR Part 313-Comment**

COMMENTS OF THE
DIRECT MARKETING ASSOCIATION, INC.

Jerry Cerasale
Senior Vice President, Government Affairs
Patricia Faley
Vice President, Consumer Affairs
The Direct Marketing Association, Inc.
Washington, D.C. 20036
202/955-5030

March 31, 2000

Counsel:

Ronald Plesser
Emilio Cividanes
Piper Marbury Rudnick & Wolfe LLP
1200 19th Street, N.W.
Washington, D.C. 20036
202/861-3900

The Direct Marketing Association (“The DMA”) welcomes this opportunity to comment on the proposed rule on the privacy of consumer financial information (“proposed regulation”) implementing Title V of the Gramm-Leach-Bliley Act.

The DMA is the largest trade association for businesses interested in direct, database, and interactive marketing and electronic commerce. The DMA represents more than 4,600 companies in the United States and 54 foreign nations. Founded in 1917, its members include direct marketers from more than 50 different industry segments, as well as the non-profit sector.

The DMA agrees that the protection of sensitive financial information should be a priority for the United States, and commends the federal banking agencies, the Securities and Exchange Commission, and the Federal Trade Commission (hereinafter collectively referred to as “the regulating agencies”) for helping advance the privacy protection that will be available in our nation by their implementation of the congressional priorities established in Title V of the Gramm-Leach-Bliley Act.

The DMA has long promoted the role that self-regulation, coupled with appropriate governmental regulation, plays in protecting consumer privacy. And The DMA continues to improve its self-regulatory efforts to empower consumers. For example, on July 1, 1999, The DMA implemented its Privacy Promise. This initiative requires that, as a condition of membership in The DMA, companies participate in The DMA’s mail and telephone preference services. These services are offered free of charge to consumers, giving them the ability to remove their names from the lists of national marketers, substantially reducing their unsolicited commercial mail and telephone marketing calls. Member companies must provide notice to consumers if they transfer data to others and must provide the consumer with the ability to opt out of such transfers. DMA members also must honor requests not to be contacted – whether from customers or prospects.

The success of the Privacy Promise is demonstrated by its widespread adoption by businesses. To date, more than 2,500 companies have signed on to the Privacy Promise. Moreover, The DMA has publicly announced the expulsion of several members that failed to comply with the Privacy Promise.

The DMA’s concerns with the proposed regulations lie primarily with their overly broad definition of the term “nonpublic personal information” (NPPI) which threatens to disrupt marketing activities not intended to be covered by Congress. We urge the regulating agencies to preserve the flow of accurate name and address information by clarifying that neither the credit bureaus’ dissemination of credit header data for marketing purposes, nor the bureaus’ use of data from financial institutions to derive credit headers, run afoul of the Gramm-Leach-Bliley Act.

In addition, we ask that the regulating agencies narrow the scope of the information subjected to the notice and opt out requirements by excluding from the definition of NPPI name and address information that merely links an individual with a financial institution, by adopting

Alternative B's definition of the term "publicly available information," and by crafting an exception for the sharing of account numbers in encrypted form for marketing purposes. Finally, the DMA asks that the regulating agencies simplify the notice and opt out requirements.

Taken together, these changes would ensure that the final regulations contain reasonable notice and opt out obligations that apply to the disclosure of only sensitive financial information.

I. Preserving the Flow of Accurate Name and Address Information

Clarify that Identifying Data from a Consumer Reporting Database May Be Used for Marketing Purposes

Compilers of marketing databases use certain identifying information from consumer reporting databases' "credit header" data to update their consumer address information. This helps ensure that marketing solicitations are not misdirected. This identifying information is often called "header information" or "above the line" information because it can be found at the top of a consumer report. These headers contain information such as name, address, previous address, and telephone number; they do not contain employment, financial, or other information residing in credit files.

Header information provides the most current address data that are commercially available because the information is partially derived from the records of creditors. Address and other identifying information that creditors possess is ordinarily more current than that available from, for example, telephone directories or even motor vehicle records, because creditors tend to communicate with their customers and update their files more frequently. When coupled with other demographic information, the result of the use of such identifying information is better targeted solicitations and more cost effective direct marketing. In short, header information increases the likelihood that consumers will receive solicitations specifically intended for them.

Financial institutions are significant suppliers of the header data used by direct marketing services. Their role as suppliers stems from the fact that they attach identifying information to the account balance and other financial data that they routinely report to consumer reporting agencies in accordance with the Fair Credit Reporting Act (FCRA).

The Federal Trade Commission has long recognized that the FCRA operates to make this identifying information available for marketing purposes,¹ and has indeed recently reiterated this view of the operation of the FCRA.² Contrary to the intent of Congress, however, the proposed

¹ See Federal Trade Commission v. TRW Inc., No. 3-91CV2661-H (N.D. Tex. Jan. 14, 1993) ("Agreed Order Amending [Dec. 1991] Consent Order").

² See In Re Trans Union (March 1, 2000).

regulations can be read to restrict the flow of identifying information obtained from a consumer reporting database. This approach to implementing Title V of the Gramm-Leach-Bliley Act rests upon reading its provisions out of context, and is neither faithful to congressional intent nor necessary to protect the privacy interests of consumers in sensitive financial information.

First, the federal agencies' concern with protecting customer lists as part of the "nonpublic personal information" does not apply to the redissemination of header information because, when redisseminated by consumer reporting agencies, these identifying data are not in a customer list form that could reveal the existence of a customer relationship with a financial institution.

A brief description of the process of "creating" a header underscores the fact that it does not reveal the existence of a customer relationship with a financial institution. Consumer reporting agencies compile information about a consumer's creditworthiness from several sources: (1) bankruptcy records, liens, court judgments, and other public records; (2) non-financial sources such as state child welfare enforcement agencies about a person's currency or arrears in his or her support payments; and (3) creditors about a consumer's performance on his or her tradelines. Using the identifying information that accompanies these sets of data, the consumer reporting agency compiles this information for a particular consumer and homogenizes the identifying information to arrive at the most accurate set of identifying information (e.g., is the street address a "Boulevard," "Avenue," or "Street"? or does the individual have a generation suffix such as "Jr."?). This identifying information is then reassembled in an individual's file as "above the line" identifying information at the top of the report distinct from "below the line" financial information filling in the rest. At this stage, the header is the product of various sources, none of which are specifically linked to it. That is, it is no longer possible at this stage to determine whether the address was obtained from a court record or a credit card account trade line, or whether the SSN was obtained from the bankruptcy court files or a mortgage loan trade line. This header is then stripped from the rest of the file in the consumer reporting database and used for other non-credit reporting products and services.

Second, restricting the flow of name and address information from headers would effectively "limit . . . the operation" of the FCRA. Yet, Section 506(c)³ makes clear Congress' intent to preserve the *status quo* in connection with the operation of the FCRA,⁴ at least in connection with permissive activities not explicitly addressed by the Gramm-Leach-Bliley Act.⁵

³ "[N]othing in this act shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act."

⁴ A basic canon of statutory construction instructs that when, as here, Congress re-enacts or borrows a statute, it incorporates settled interpretations of that statute.

⁵ Another canon of statutory construction directs that provisions which only generally cover an issue yield to more specific provisions that target a particular issue.

In the absence of a specific provision targeting the particular issue of the redissemination of header data, section 506(c)'s scope extends to court orders and federal agency interpretations recognizing that the FCRA operates to allow the marketing use of this identifying information from a consumer reporting database.⁶

In short, when read together, sections 502(c), 502(e)(6), and other provisions of the Act do not restrict the redissemination of identifying information obtained from a consumer reporting database. The final regulations should make this clear.

Nevertheless, some financial institutions may interpret section 502(c)'s limitations on the redisclosure and reuse of information as requiring them to contractually restrict consumer reporting agencies from redisseminating credit header information. Consequently, the final rule also should reassure financial institutions that the *status quo*—*i.e.*, the marketing uses of identifying data supplied by them to consumer reporting agencies—does not run afoul of the Gramm-Leach-Bliley Act. Indeed, it should clarify that a financial institution's attempt at restricting the redissemination of header information impermissibly limits the operation of the FCRA.

Exclude Customer Lists from NPPI

The goal of the rigorous notice and opt out safeguards of Title V of the Gramm-Leach-Bliley Act is the protection of sensitive financial information. As indicated in section 501, the protection of “nonpublic personal information” (NPPI) entails protecting financial information “which could result in substantial harm or inconvenience” to an individual.

Nevertheless, the regulating agencies propose imposing burdensome notice and opt out obligations on information that reveals merely the fact of a customer relationship between an individual and a financial institution. The proposed regulation explicitly states that “[t]he fact that that an individual is or has been one of a [financial institution's] customers or has obtained a financial product or service from a [financial institution]” falls within the definition of NPPI. This is inconsistent with the Act. The final rule should reject this approach and instead make clear that the disclosure of a list of financial institution customers is not subject to the same rigorous safeguards that apply to truly sensitive financial information.

⁶ See, e.g., Federal Trade Commission v. TRW Inc., No. 3-91CV2661-H (N.D. Tex. Jan. 14, 1993) (“Agreed Order Amending [Dec. 1991] Consent Order”); Trans Union Corp. v. Federal Trade Commission, 81 F.3d 228, 232 n. 1 (D.C. Cir. 1996) (citing 1993 amendment to TRW consent decree); In Re Trans Union ___ FTC ___ (March 1, 2000).

First, the disclosure of the existence of a customer relationship with a financial institution is not the type of financial information “which could result in substantial harm or inconvenience” to an individual.⁷

Second, given the vast diversity of financial products and services that any one financial institution can now offer, the disclosure of the existence of a customer relationship with a particular financial institution reveals virtually nothing about the type of financial product or service that a consumer has purchased from such institution.⁸ Indeed, the departure from Congress’ intent is compounded when this broad definition of NPPI is coupled with the broad definition of “financial institution” promulgated by the FTC. The result is that retailers such as L.L. Bean can be deemed to be “financial institutions,” a list of their customers can be deemed to be NPPI, and any intention to disclose their customer lists can trigger the notice and opt out requirements of Title V of the Gramm-Leach-Bliley Act.

Applying the proposed regulation’s rigorous notice and opt out requirements to customer lists effectively reads the term “financial” out of the statutory definition of NPPI even though Congress defined the term with care, differentiating protected information from other data by requiring that protected information be, *inter alia*, “financial” as well as “personally identifiable.”

Moreover, customer lists are protected under The Direct Marketing Association’s industry guidelines and Privacy Promise, which require its member companies to furnish customers with notice and an opportunity to opt out from the distribution of customer lists for marketing purposes.

Finally, the inclusion of customer list information in the definition of NPPI undermines the goal of giving meaning to the statutory exclusion for “publicly available information,” as contained in Alternative B’s definition of the term (see below).

Adopt Alternative B’s Definition of the Term “Publicly Available Information”

Congress excluded “publicly available information” from the type of sensitive financial information covered by the definition of NPPI. This reflects, in part, the U.S. Supreme Court’s often stated rule that people are free to use personally identifiable information that is in the public domain.

⁷ We submit that, in many if not most instances, other customer list information in addition to names and addresses also is not intrinsically financial in nature.

⁸ Indeed, under the proposed rule’s notice requirement, any reference to “financial products or services” is vague unless followed by illustrations of the lines of business.

As proposed by the Federal Reserve Board in so-called Alternative B, the final rule should define “publicly available information” to mean the type of information that is lawfully made available to the general public in public records and publicly available publications. This approach reflects a deeper understanding that, in multi-source records, it is nearly impossible to determine accurately the source of any specific data element and, more importantly, the financial burdens and inefficiencies of attempting to do so.

In its current form, however, Alternative B does not go far enough in effectuating Congress’ intent to exclude all information that is lawfully publicly available. As proposed, Alternative B would permit publicly available information to be treated as NPPI if the information is derived using a financial institution’s customer list. The inclusion of customer list information in the definition of NPPI renders the differences between Alternatives A and B virtually meaningless in the context of lists of consumers. To give meaning to the statutory exclusion for “publicly available information” in all contexts, the final rule should exclude customer lists from the definition of NPPI.

The FTC has proposed a variation of Alternatives A and B. Alternative B is preferable to the FTC’s proposal. The FTC’s proposal would require financial institutions to undertake reasonable procedures to establish that information is, in fact available from public sources before the financial institution may treat it as “publicly available information.” As noted above, this can be costly and inefficient. To the extent that the FTC’s proposal would require financial institutions to undertake nearly the same level of effort as would be required by Alternative A, it should be rejected because it would blur the principal distinction between Alternatives A and B.⁹

II. Adopt an Exception for the Sharing of Account Numbers in Encrypted Form

The Notice of Proposed Rulemaking asks for comments on whether it is appropriate for the final regulation to include an exception to Section 502(d) of the Gramm-Leach-Bliley Act, which prohibits financial institutions from disclosing account numbers and similar access codes to nonaffiliated third parties for marketing purposes. Section 502(d) serves to prevent account numbers and similar information from being used to access a consumer’s account without the consumer’s knowledge. The DMA believes that the regulating agencies should craft a narrow exception that recognizes a consumer’s right to consent to the transfer of such information, particularly in encrypted form.

The fact is that Section 502(d), and its counterpart in the proposed regulation, is extraordinary insofar as it prohibits the disclosure of a consumer’s information irrespective of his or her consent. Privacy laws tend to focus on the *unconsented* collection and disclosure of personal information; they invariably authorize the targeted practices whenever the consumer has

⁹ If, on the other hand, the FTC’s proposal would enable a financial institution to use information once it has been filtered against, for example, a national listing of unpublished telephone numbers, then the proposal is at least preferable to Alternative A.

consented to them. Even our wiretap laws, which are grounded in our Bill of Rights, authorize electronic surveillance with a party's consent.¹⁰ So does the Right to Financial Privacy Act,¹¹ which was enacted in response to a Supreme Court decision that the Fourth Amendment did not require law enforcement agencies to secure legal process in order to obtain from a bank the financial records of a depositor.¹² It would be ironic and “National Nanny” in the extreme if a customer can consent to a financial institution's disclosure of his or her personal financial information to government investigators but cannot consent to such disclosures when they are for the purpose of providing the customer with a product or service that he or she has chosen.

The Congress recognized both the breadth of section 502(d) and the difficulty of statutorily crafting an appropriate exception to it. Consequently, the Managers of the Conference encouraged the regulating agencies to craft an exception to section 502(d) to permit disclosures in limited circumstances,¹³ and the Congress gave the regulating agencies the statutory authority to do so.¹⁴ This was reiterated in floor debate by the Banking Committee Chairman and the Chairman and Vice Chairman of the Financial Institutions Subcommittee during the Senate's consideration of the Conference Report,¹⁵ and in a subsequent bipartisan letter from members of the Senate Banking Committee.¹⁶

The final regulation should enable financial institutions to disclose account numbers in encrypted form to third parties for marketing purposes only if the third party is required to obtain the customer's affirmative consent to be billed to that account prior to decrypting the account information. This both respects the consumer's right to consent to the transfer of account information and safeguards customer financial information. It safeguards the customer's

¹⁰ See, e.g., 18 U.S.C. § 2511(2)(d) (consent of one of the parties to the communication); Md. Code Ann. § 10-402(c)(3) (consent of all parties to the communication). If there are concerns that the consumer could be coerced into giving his or her consent, then statutory or regulatory restrictions focus on prohibiting the entity from conditioning a service on a consumer's consent to the targeted practice. See, e.g., 15 U.S.C. § 6502(b)(1)(C) (Children's Online Privacy Protection Act); 64 Fed. Reg. 60055 (Nov. 3, 1999) (proposed 45 C.F.R. § 164.508(a)(2)(iii) protecting the privacy of patients' health information).

¹¹ See 12 U.S.C. § 3404 (customer authorizations).

¹² See H.R. Rep. No. 1383, 95th Cong., 2d Sess. 6 & 33, *reprinted in* 1978 U.S. Code Cong. & Admin. News 9273, 9278 & 9305 (congressional response to United States v. Miller, 425 U.S. 435 (1976)).

¹³ See H.R. Rep. No. 434, 106th Cong., 1st Sess. 173 (1999) (Conference Report to S. 900) (Managers' Statement).

¹⁴ See 15 U.S.C. § 6804(b) (agency authority to grant exceptions).

¹⁵ See 146 Cong. Rec. 13902 (Nov. 4, 1999) (colloquy between Sens. Gramm, Bennet, and Hagel).

¹⁶ See Letter to John D. Hawke, Jr., from Sens. Gramm, Bennet, Hage, Johnson, and Bayh (December 22, 1999).

financial information because the encrypted account number cannot be used by the third party to access the customer's account. It respects the customer's right to consent to the transfer because it enables the third party to decrypt the account number and access the customer's account only with his or her consent.

This use of encrypted account numbers ensures accuracy, improves the cost efficiency of the billing process, and reduces the potential for fraud by eliminating the need to ask for the customer's account number (and for the customer to get in the habit of furnishing it via telephone).

III. Making the Notice and Opt Out Obligations More Reasonable

Some of our members inform us that compliance with the proposed regulation will increase the length of their privacy notices by as much as 300%, for example, expanding a two-page privacy notice into an eight-page notice. Unless privacy notices under the Gramm-Leach-Bliley Act are kept simple and short, consumers will tend not to read them because the notice will be "just another legal document" about matters consumers cannot affect, instead of a disclosure of relevant practices, some of which the consumer can choose not to participate in.

The Importance of Keeping the Privacy Notice Simple and Concise

Consumer privacy notices tend to inform consumers how to exercise opt out rights while still transacting business with the company furnishing the notice. By comparison, the disclosure statements in legal documents used, for example, in the closing of a mortgage loan, furnish consumers with little choices other than scuttling the transaction.

Consequently, the goal of a privacy notice has been to furnish meaningful disclosure of those practices undertaken by an entity that materially affect a consumer's privacy interests. However, as noted by a federal court of appeals reviewing the subscriber privacy requirements of the 1984 Cable Act: "The virtue of 'meaningful disclosure' is lost when the inclusion of too much information 'result[s in] a piece of paper which appears to be 'just another legal document' instead of the simple, concise disclosure form Congress intended.'"¹⁷

The importance that these privacy notices focus on providing meaningful disclosure—and not be required to provide additional information that is redundant or marginally useful to the average consumer—is highlighted by the timing of the first set of privacy notices required by the Gramm-Leach-Bliley Act.

- On or about December 16, 2000, consumers will be deluged with privacy notices from all of the financial institutions with which they do business.

¹⁷ Scofield v. TeleCable of Overland Park, Inc., 973 F.2d 874, 880 (10th Cir. 1992).

- This means that an average family could simultaneously receive privacy notices from two or more credit card companies, several department stores where they enjoy charge card privileges, two or more banks and credit unions, their brokerage house, their financial planner, their travel agent, and, possibly, their various insurance companies.
- And, if the family purchases a computer, furniture, car, or home, they could also within weeks of December 16 also receive privacy notices from the computer manufacturer, the furniture retailer, the car company, and the real estate appraiser.

If the notices look like “just another legal document”, consumers will likely discard the notices without reading them and thereby undermine the congressional goals of Title V of the Gramm-Leach-Bliley Act.

Simplify the Privacy Notice

The proposed regulation’s examples tend to undermine the concise privacy notice contemplated by Title V of the Gramm-Leach-Bliley Act.

For example, whereas the Act requires disclosure of the “categories” of NPPI that may be disclosed, and the “categories” of persons to whom the NPPI may be disclosed, the proposed regulation requires notice of far greater detail. Under the proposed regulation:

- It does not suffice for a financial institution to inform consumers that the “categories” of information that it may disclose include “identifying information.” Rather, the financial institution is required to enumerate items of information, such as “name, address, social security number.”
- It does not suffice for a financial institution to inform consumers that the “categories” of persons to whom it may disclose NPPI include “magazine publishers.” Rather, the financial institution is required to identify them as “companies engaged in selling *investment*-related magazine subscription products”, and to differentiate these publishers from “companies engaged in selling *health*-related magazine subscription products.”

Another example of unnecessary detail is the proposed regulation’s notice requirements in connection with the exception to opt out requirements for service providers and joint marketing.

- The Act merely requires that financial institutions “fully disclose” “the providing of such information”—*i.e.*, the fact that NPPI is provided for such purposes.
- The proposed regulation reads this substantive disclosure obligation to require in each notice “a separate description” of the “categories of information that are disclosed *and* the categories of third parties providing the services.”

- This unnecessary requirement is further compounded by, as discussed above, the unnecessary level of detail that is being required to satisfy the “categories” requirement.

The opt out requirements further illustrates the proposed regulation’s unnecessary prescriptiveness.

- Where the Act requires that financial institutions notify consumers of the fact that NPPI may be disclosed to a nonaffiliated third party, the proposed regulation requires the institution to enumerate “all” of the “categories” of NPPI that are, or may be, disclosed to nonaffiliated third parties.
- Where the Act requires that financial institutions give consumers “an explanation” of how they can exercise their opt out right, the proposed regulation requires the institution to provide the consumer with an opt-out package: privacy notice with detachable opt out form and a self-addressed envelope.

Conclusion

The DMA urges the regulating agencies to ensure that the final regulation contains reasonable notice and opt out obligations that apply to the disclosure of only sensitive financial information.