October 9, 2001

VIA HAND DELIVERY

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

Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule
16 C.F.R. Part 313–Comment

Dear Mr. Secretary:

The following comments are submitted on behalf of the ACA International ("ACA") in response to the Federal Trade Commission's ("Commission") request for comments on the proposed rulemaking to implement the administrative, technical and physical information safeguards for financial institutions subject to the Commission's jurisdiction under the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801 *et seq.* *See* Standards for Safeguarding Customer Information, 66 Fed. Reg. 41162 (Aug. 7, 2001) (hereinafter "Proposed Rule"). ACA has enclosed five copies of the comments, along with a computer disk containing ACA's comments saved in PDF format. These comments supplement the comments filed with the Commission on Oct. 3, 2000, in response to the Commission's request for comments on the Advance Notice of Proposed Rulemaking. *See* Privacy of Customer Financial Information – Security, 65 Fed. Reg. 54186 (Sept. 7, 2000) (Advance Notice of Proposed Rulemaking and Request for Comment).

I. Statement on ACA

ACA International, formerly known as American Collectors Association, Inc., is a trade association of credit and collection professionals who provide a wide variety of accounts receivable management services. Headquartered in Minneapolis, Minnesota, ACA represents approximately 5,300 third-party collection agencies, attorneys, credit grantors and vendor

4040 WEST 70TH STREET 55435 P.O. BOX 39106 MINNEAPOLIS, MN 55439-0106
TEL (952) 926-6547 FAX (952) 926-1624 ACA@COLLECTOR.COM HTTP://WWW.COLLECTOR.COM

affiliates. Some ACA members also participate in ACA's Asset Buyers Program ("ABP").[1] The Asset Buyers Program caters to members that purchase debt from third party creditors. The sale and purchase of accounts receivables continue to be a thriving aspect of the collection industry. In 2000 alone, creditors sold more than $27 billion of debt to third parties.

II. Comments on the Proposed Rule

ACA compliments the Commission on adopting a flexible approach to the Proposed Rule allowing financial institutions discretion to create procedures reasonably tailored to their business operations. Flexibility is warranted based on the divergent impact that the Proposed Rule will have on ACA members ranging in size from small businesses with a few employees to multi-state corporations with thousands of employees. Moreover, the flexibility recommended by the Proposed Rule is consistent with the guidelines issued by the various banking agencies that have promulgated similar security rules. ACA's specific comments on the Proposed Rule are as follows:

A. 16 C.F.R. § 314.1(b) – Recipient Financial Institutions

Section 314.1(b) states that the Proposed Rule "applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you." As such, the Commission proposes to expand the scope of the Proposed Rule to include not only a financial institution's handling of its own customers' information, "but also financial institutions that receive customer information from other financial institutions." 66 Fed. Reg. at 41164. The Commission justifies this approach based on its belief that "including recipient financial institutions within the rule will assure greater safeguards for customer information and is within the authority conferred by the Act." ACA respectfully disagrees that Congress intended this result or extended a legislative grant of authority to this end.

We find no support in the GLBA for the Commission's expansion of the scope of the Proposed Rule to include disclosures of customer information by a financial institution to another institution that has no customer relationships. To the contrary, a plain reading of the

---

[1] ACA's comments are submitted primarily in contemplation of the Proposed Rule's application to ABP members because these businesses are most directly regulated by GLBA. Although collection agencies are financial institutions within the meaning of GLBA, *see Privacy of Consumer Financial Information*, 65 Fed. Reg. 33646 (May 24, 2000) (*codified* at 16 C.F.R. § 313 *et seq.* (2000)), the Commission has clarified that "[a] consumer has a 'customer relationship' with a debt collector that purchases an account from the original creditor (because he or she would have a credit account with the collector), *but not with a debt collector that simply attempts to collect amounts owed to the creditor.*" 65 Fed. Reg. at 33653 n. 18 (citation omitted) (emphasis added). Consequently, ACA's ABP members that purchase receivables and locate the debtor *and* attempt to collect payment may have a compliance obligation, *see* 65 Fed. Reg. at 33653, while third-party collection agencies must mainly be concerned with the GLBA reuse and redisclosure requirements.

Commission's authority to create the Proposed Rule holds otherwise. The policy set up by Congress states:

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the *privacy of its customers* and to protect the security and confidentiality of those customers' nonpublic personal information.

15 U.S.C. § 6801(a) (emphasis added). The statute clearly refers to "customers" – the customers specific to the financial institution with the affirmative obligation to protect the security and confidentiality of customer information.[2] The Proposed Rule re-writes this provision to declare the "policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the *privacy of ALL customers*," regardless whether the customer is, in fact, a customer of the financial institution. If Congress would have intended this policy result, it would have so specified.

The Commission's interpretation also blurs the distinguishing characteristics between "customers" and "consumers" as those terms are defined in the Commission's Final Privacy Rule, Privacy of Consumer Financial Information, 16 C.F.R. § 313 *et seq.* The GLBA requires the Commission to "establish appropriate standards for the financial institutions . . . relating to administrative, technical, and physical safeguards (1) to insure the security and confidentiality of ***customer records and information***; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any ***customer***." 15 U.S.C. § 6801 (b) (emphasis added). Further, 15 U.S.C. § 6801(a) declares the congressional policy that financial institutions have an affirmative and continuing obligation to "respect the privacy of its ***customers*** and to protect the security and confidentiality of those *customers' nonpublic personal information*. . . ." 15 U.S.C. § 6801(a) (emphasis added). By broadening the scope of the Proposed Rule to include financial institutions that receive customer information from other financial institutions, the Proposed Rule transforms the safeguard provisions to include not just "customers," but also "consumers." This is because "customer"[3] information in the hands of third-party financial institutions is "consumer"[4] information under the Final Privacy Rule since the recipient financial institution has no "customer relationship"

---

[2] Congress instructed the Commission to create the safeguard provisions "in furtherance of the policy in subsection (a) of this section," that is, based on a financial institution's affirmative and continuing obligation to protect *its customers'* privacy.

[3] A "customer" is a "consumer" who has a "customer relationship" with the financial institution. 16 C.F.R. § 313.3(h). In turn, "customer relationship" 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 that are to be used primarily for personal, family, or household purposes. 16 C.F.R. § 313.3(h)(i).

[4] A "consumer" is defined as "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative." 16 C.F.R. § 313.3(e)(1).

with the underlying consumer. This is not what GLBA directs. The scope of the safeguard provisions was intended to only apply to "customers" of financial institutions, and not "consumers" generally.

B. 16 C.F.R. § 314.1(b) – Compliance With HIPAA

The Commission also requests comment on whether and how compliance with other laws and rules relating to information security should be addressed in the Proposed Rule, including the rules relating to medical information under the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, *see* "Standards for Privacy of Individually Identifiable Health Information," 65 Fed. Reg. 82462 (Dec. 28, 2000) (*codified at* 45 C.F.R. § 164 *et seq.* (hereinafter "HIPAA Rule")). ACA believes that the Proposed Rule should be consistent with the comprehensive security standards set forth in the HIPAA Rule. Further, the Commission should accept ACA members' compliance with the HIPAA Rule security standards as full compliance with the Proposed Rule.

Collection agencies are not "covered entities" under the HIPAA Rule. However, agencies collecting medical debts access "protected health information" – a term equivalent to "nonpublic personal information" in GLBA. Consequently, under the HIPAA Rule, ACA members are "business associates" or "healthcare clearinghouses" because they collect healthcare receivables, such as co-pays, deductibles and out-of-pocket payments.

The Department of Health and Human Services ("HHS") has proposed rigorous security standards that apply to covered entities and healthcare clearinghouses. *See* "Security and Electronic Signature Standards," 63 Fed. Reg. 43242 (Aug. 12, 1998) (proposed rule).[5] The security standards protect the confidentiality and integrity of individually identifiable health information. HHS proposes to do so by creating substantial protections covering the physical protection of information in terms of storage and maintenance. It also addresses technical requirements to implement the standards including restricted access, computer networks, user identification and other protections. In summary, the security standards proposed by HHS meet and exceed those in the Proposed Rule. Based on these comprehensive standards, compliance with HIPAA's security standards should satisfy any compliance obligation of a financial institution under the Proposed Rule.

Indeed, simply adding another layer of redundant security standards will not foster any greater protections to the privacy of customers' information. This is especially true in the case of the collection industry. Federal and state privacy laws and regulations governing the collection industry already provide comprehensive privacy protections such as those reflected in the GLBA. For example, ACA members are regulated by the Fair Debt Collection Practices Act, 15

---

[5] HHS has not issued a final rule implementing the security standards. Collection agencies collecting medical debt will be governed by the HHS security standards either directly as healthcare clearinghouses or indirectly based on the standards established for processing information through third parties. According to HHS, such third parties will be required to enter into a chain of trust partner agreements. These are contracts in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information.

U.S.C. § 1692 *et seq.* ("FDCPA"). Among other aspects, the FDCPA delineates the proper procedures for obtaining debtor location information, communicating with consumers, and disclosing that consumers have the right to dispute the validity of the debt. The FDCPA includes provisions that not only regulate the communication between debt collectors and consumers, but also regulate communication between debt collectors and third parties. Only in very limited situations may a debt collector communicate with anyone other than the consumer, as defined by the statute. Certain provisions of the FDCPA restrict "communications"[6] by "debt collectors"[7] in connection with the collection of a debt.

In addition to the FDCPA, other federal laws governing collection agencies restrict access to nonpublic personal information. For example, collection agencies that "furnish" consumer information to consumer reporting agencies are governed by the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA"). This law contains express limitations on the type of consumer information that can be disclosed to third parties.[8] Moreover, the majority of states have adopted specific debt collection and privacy laws.

C. 16 C.F.R. § 314.2(b) – Customer Information

The Commission acknowledges that the Proposed Rule is limited to "'customer information' and not to information about other consumers who do not meet the definition of 'customer.'" 66 Fed. Reg. at 41165. And still it states that "protecting information about consumers may be a part of providing reasonable safeguards to 'customer information' where the two types of information cannot be segregated reliably." *Id.* In substance, the Commission suggests that compliance may depend in some cases on the protection afforded consumers, as opposed to customers. While this may be a consideration under the Commission's jurisdiction pursuant to section 5 of the Federal Trade Commission Act to regulate unfair or deceptive acts or practices in or affecting commerce, 15 U.S.C. § 45(a)(1), it is not an approach supported by GLBA. By the terms of GLBA, the safeguard standards are limited to "customer" information. *Id.* & n. 38 (citing section 501(a) &

---

[6] The FDCPA broadly defines communication as "the conveying of information regarding a debt directly or indirectly to any person through any medium." 15 U.S.C. § 1692a(2).

[7] A "debt collector" is defined as "any person who uses any instrumentality of interstate commerce or the mails in any business the principal purpose of which is the collection of any debts, or who regularly collects or attempts to collect, directly or indirectly, debts owed or due or asserted to be owed or due another." 15 U.S.C. § 1692a(6).

[8] The FCRA prohibits furnishers of consumer information from providing information to a consumer reporting agency that they know, or consciously avoid knowing, is inaccurate. 15 U.S.C. § 1681s-2(a)(1). When a consumer notifies the furnisher of a perceived inaccuracy which is then verified, the correct information must be forwarded to the consumer reporting agency. 15 U.S.C. § 1681s-2(a). Moreover, if a consumer reporting agency notifies the furnisher of a consumer's dispute of the accuracy of information provided by the furnisher, the furnisher must conduct an investigation of all relevant information provided by the consumer reporting agency, as well as any material given to the agency by the consumer, and report the results of the investigation to the agency. 15 U.S.C. § 1681s-2(b).

(b)(1)-(3)). The Commission's evaluation of the "reasonableness" of a financial institution's safeguarding of such customer information should not be tied to protections against consumer information disclosures.

D. 16 C.F.R. § 314.4(d) – Contracting with Service Providers

The Proposed Rule seeks to require financial institutions to enter into contracts with service providers to implement and maintain customer information shared with the service provider. 16 C.F.R. § 314.4(d). The Commission asks for comment on this contracting requirement. ACA believes that requiring contracts to implement and maintain the safeguard standards is unnecessary where the recipient service provider is, itself, a financial institution, and unwarranted under GLBA where the recipient service provider receives nonpublic personal information ("NPPI") pursuant to the exemptions in sections 313.14 and 313.15.

In many instances, a financial institution functioning as a service provider that comes into possession of NPPI may trigger GLBA's compliance requirements. There is no basis for the Commission to further cement the privacy protections by requiring financial institutions that share such NPPI with recipient financial institutions to enter into contractual arrangements merely to codify obligations already existing under federal law. Thus, the Proposed Rule should exempt from the contracting requirement financial institutions that have an existing GLBA safeguard compliance obligation.

Nor do we see a basis to impose a contracting requirement in cases where a service provider receives customer information pursuant to a GLBA exemption. The Commission correctly notes that "*the Privacy Rule does not require financial institutions to enter into confidentiality contracts with service providers* that received information under the general exceptions in sections 313.14 and 313.15 of the rule." 66 Fed. Reg. at 41166 (emphasis added). If the Commission's final privacy rule does not require contracting between service providers and financial institutions based on these exemptions, we believe that consistency with the final privacy rule requires that the Proposed Rule exempt from the contracting requirement information shared pursuant to a GLBA exemption.

Moreover, even if a service provider receives NPPI, there is a remedy for privacy infringements without imposing complex contracting requirements that essentially cede the Commission's obligation to enforce GLBA to the private sector. That remedy, of course, is section 5 of the Federal Trade Commission Act, in addition to other privacy statutes enforced by the Commission such as the FCRA and the FDCPA.

E. 16 C.F.R. § 314.5 – Effective Date

The Proposed Rule requires financial institutions to implement their information security programs within one year of the date in which a final rule is announced. ACA believes that the complexity of the Proposed Rule warrants a phased implementation, similar to the Commission's treatment of the final privacy rule.[9] As currently proposed, financial institutions will be strained

---

[9] The Privacy Rule became effective on Nov. 13, 2000, but the Commission extended the period for full compliance until July 1, 2001.

to take the steps necessary to comply with the Proposed Rule, such as (1) identifying internal and external security risks, (2) train employees and management, (3) update or obtain entirely new information systems capable of processing, storing and disposing of information, (4) develop response measures to attacks and security intrusions, (5) test the security measures, and (6) work with service providers and, if required, implement new contracts.[10] Substantial work will be required to implement these measures. The burdens on small businesses members of ACA will be profound. These businesses should not be impeded in their operations as they come into compliance. Consequently, we propose that the security measures become effective one year after the date in which the final rule is announced, but affected business should be given an additional 12 months before full compliance is required.

F. Questions for the Commission

ACA members request that the Commission respond to several questions concerning the practical effects of the Proposed Rule, as follows:

1. Please confirm that financial institutions are not required to submit their safeguard procedures or policies to the Commission or make them available to consumers.

2. The Commission's Privacy Rule required financial institutions to make a general disclosure to consumers with respect to the safeguard procedures. *See* Sample Clause A-7. Is this Sample Clause still effective? Can financial institutions still rely on it? If a financial institution previously has sent privacy notices using the Sample Clause, are new privacy notices required when the Proposed Rule becomes effective?

3. Does the Commission expect financial institutions to monitor or test the security procedures utilized by service providers that receive NPPI?

4. What is a "system attack" as that term is used in section 314.4? Does this mean hacking into a database? What about computer viruses?

---

[10] The Commission also should grandfather any contracts with service providers as provided for section 313.18(c) of the Privacy Rule.

III. Conclusion

ACA appreciates the Commission's consideration of these comments. We commend the Commission's effort to adopt flexible standards that make sense for business and consumers. If you have any questions about ACA's comments, please contact:

Glenn A. Mitchell, Esq.
Andrew M. Beato, Esq.
ACA Federal Regulatory Counsel
1100 Connecticut Avenue, NW, Suite 1100
Washington, D.C. 20036
(202) 737-7777

Respectfully submitted,

Gary D. Rippentrop, CAE
Chief Executive Officer
ACA International
P.O. Box 39106
Minneapolis, MN 55439-0106
(952) 926-6547

Glenn A. Mitchell, Esq.
Andrew M. Beato, Esq.
ACA Federal Regulatory Counsel
1100 Connecticut Avenue, NW
Suite 1100
Washington, DC 20036
(202) 737-7777