(1 A)

American Financial Services Association
919 Eighteenth Street, NW • Washington, DC • 20006
phone 202 296 5544 • fax 202 223 0321 • email afsa@afsamail.org
www.americanfinsvcs.org

The Market Funded Lending Industry

August 25, 2000

2000 AUG 28 A 8:50

Communications Division
Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Re: Docket No. 2000-51

Dear Sir or Madam:

The American Financial Services Association ("AFSA") is the trade association for approximately 360 non-traditional market-funded providers of financial services to consumers and small businesses. It was founded in 1916. AFSA members have over 10,000 offices in the United States with outstanding receivables of over $200 billion. Market funded lenders provide between 15% and 20% of all consumer credit in the United States.

AFSA appreciates the opportunity to comment on the proposed interagency Guidelines establishing standards for safeguarding customer information, promulgated under Section 501 of the Gramm-Leach-Bliley Act ("GLB Act"). AFSA recognizes and appreciates the Agencies' effort to implement these important information security provisions of the GLB Act.

As an initial matter, AFSA commends the Agencies' focus in the proposed Guidelines on the process financial institutions should employ in developing standards for safeguarding customer information and information security programs. The emphasis on procedural issues, such as undertaking a risk assessment, developing a risk management plan and requiring Board of Directors approval and oversight, should be retained. The Agencies should not shift their focus to specify substantive requirements that would be difficult to apply uniformly across the range of financial institutions subject to the Guidelines.

AFSA provides the following comments to assist the Agencies in developing Guidelines that satisfy the requirements of Section 501 of the GLB Act.

Comprehensive Risk Management Plan

The proposed Guidelines provide that a financial institution shall, as part of a comprehensive risk management program, establish written policies and procedures to control identified risks and achieve the overall objectives of its information security program. The Agencies further propose that in establishing these policies and procedures, a financial institution "should consider appropriate" access rights, controls, restrictions, encryption, contract provisions and the like.

We believe that it is the Agencies' intent that the list of safeguards in the proposed Guidelines are a series of possible safeguards that a financial institution should consider in light of risks it has identified, the nature of the information, etc. However, the language "should consider appropriate" could be construed to indicate that the Agencies are suggesting that a financial institution must implement each item listed. We urge the Agencies to make clear their intent that the list is a series of safeguards that should be considered by financial institutions, and adopted only as the financial institutions deem appropriate in light of their identified risks.

Encryption

The proposed Guidelines provide that in establishing a risk management program, a financial institution should consider as part of this program appropriate "encryption" of customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access. The Agencies should make it clear in the Guidelines that a financial institution is not required to encrypt customer information wherever stored or each time the data is transmitted to a service provider or other third parties. Encryption procedures are expensive for financial institutions to implement and may be unwarranted depending on, among other things, the sensitivity of the type of data and the degree of risk that unauthorized individuals may have access to the data. A financial institution should be provided the flexibility under the Guidelines to decide when it is appropriate to use encryption technology.

Access Rights

The proposed Guidelines describe the elements of a comprehensive risk management plan designed to control identified risks and to achieve the overall objective of ensuring the security and confidentiality of customer information. In doing so, the proposed Guidelines state that in establishing a risk management program, a financial institution should consider as part of this program appropriate "access rights" to customer information, among other things.

The reference to "access rights" should be deleted. Section 501 does not create any independent substantive right of customers to have "access" to information that relates to them, nor do the final Privacy Rules impose access requirements. On the other hand, to the extent that the reference to "access rights" is not intended to create "access rights" for customers, but instead is intended to suggest that a financial institution should consider

placing access controls on customer information systems, such as restricting access to customer information to properly authorized employees, the Agencies should revise this reference in the Guidelines to clarify this intent.

Outsourcing Arrangements

The proposed Guidelines state that a financial institution must exercise appropriate due diligence in "managing and monitoring" its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with the Guidelines.

The Agencies should make it clear in the Guidelines that financial institutions are not required to affirmatively audit the activities of its service providers to ensure that they have implemented an effective information security program. Instead, it should be sufficient for a financial institution to contractually require its service providers to implement information security programs and then to enforce those contractual provisions to the extent necessary. A financial institution cannot be expected to audit every service provider to ensure that such parties are complying with the Guidelines, but should be permitted to enforce contractual obligations should violations occur.

Also, in promulgating the Guidelines, the Agencies should not set forth specific contract provisions that financial institutions would be required to include in their contracts with service providers in connection with the security of information. A financial institution should have the flexibility to determine how best to craft its contract provisions with its service providers to ensure that the service providers are adequately ensuring the security of customer information. Given the breadth and variety of services that may be performed by third parties on behalf of financial institutions, the financial institutions themselves are best able to determine what contractual provisions are appropriate, and they should be given the flexibility to do so.

Elsewhere in the proposed Guidelines, the Agencies indicate that a financial institution continues to be responsible for safeguarding customer information even when it gives a service provider access to that information. This language seems to create strict liability for financial institutions for any failure of a service provider to "safeguard" customer information, even beyond the requirements of the Guidelines, and in derogation of traditional contract and tort principles. We urge the Agencies to temper this language by making it clear that financial institutions are responsible for protecting customer information *consistent with the Guidelines*, both with respect to its activities and those of its service providers.

Business Customers

The proposed Guidelines define the term "customer" to mean a customer of a financial institution as defined in the final Privacy Rules. Thus, the term "customer" for purposes of the proposed Guidelines does not include business customers or consumers who have not established an ongoing relationship with the financial institution. The Agencies then

request comment on whether the scope of the Guidelines should apply to records regarding: (i) all consumers (regardless of whether they are ongoing customers); (ii) both consumer and business customers of the institution; or (iii) all of an institution's records regardless of to whom or what they relate.

The Agencies should limit the scope of the Guidelines to apply only to customer information relating to consumers. More specifically, the Agencies should not expand the scope of the Guidelines to apply to business customers of financial institutions. Congress - in passing the privacy provisions in Title V of the GLB Act, including Section 501 - did not intend to extend the coverage of the Act to business customers of financial institutions. Furthermore, the inclusion of business customers within the scope of the Guidelines would be a significant burden on financial institutions' GLB Act implementation efforts, given that many financial institutions have different systems platforms for their consumer and business services.

Consumers and Customers

The Agencies should not expand the scope of the Guidelines to cover records regarding consumers who are not also customers. As the Agencies recognized in the final Privacy Rules that implement Section 502 and 503 of the GLB Act, Congress distinguished in the privacy provisions of the GLB Act between "customers" (*i.e.*, those individuals that have an ongoing relationship with a financial institution) and other "consumers" (*i.e.*, those individuals that have obtained a financial good or service from a financial institution for personal, family or household purposes, but that have not established an ongoing relationship). By using the term "customer," Congress clearly intended the obligations of Section 501 to apply only to individuals with whom a financial institution has an ongoing relationship. Requiring a financial institution to apply the Guidelines to the records of all "consumers" would impose additional responsibilities on financial institutions that are not mandated by Section 501.

Also, though financial institutions ultimately may decide to adopt similar security standards for all "consumer" information regardless of whether it is "customer" information, requiring an institution to do so could expose financial institutions to liability under state laws. For example, financial institutions that fail to meet the obligations in the Guidelines may be subject to "unfair business practices" claims under state law. Expanding the Guidelines to apply to "consumer" information - even where that information does not relate to "customers" - could increase a financial institution's exposure to liability as a result of such claims, where Congress intended otherwise.

Guidelines

In the Supplemental Information, the Agencies solicit comment on whether the final security standards should be issued in the form of Guidelines or as regulations. Issuing the security standards as Guidelines, instead of regulations, would provide financial institutions with the additional flexibility they need to establish an information security program that is appropriate for that individual institution, while also providing

institutions with the proper guidance they need to structure their information security programs. If an Agency, through its examinations of an individual institution, finds that the institution has not adopted adequate safeguards to protect customer information, the Agency already has the authority to impose more specific information security requirements on that institution.

Customer Information Systems

The proposed Guidelines define the term "customer information system" to mean "electronic or physical methods used to access, collect, store, use, transmit and protect customer information." Virtually any activity undertaken by a financial institution would fall within such a broad definition of "customer information system" because most of a financial institution's activities, at least in some way, involve either electronic or physical methods for accessing, collecting, storing, using or transmitting customer information. The Agencies should take a measured approach as to the extent to which customer information systems are subject to the Guidelines, depending on the nature of the information on those systems and the risks that may threaten the security, confidentiality, or integrity of customer information. Furthermore, financial institutions should have the flexibility to first implement the requirements set forth in the final Guidelines with respect to those customer information systems which involve the greatest risk, and develop policies and procedures relating to those customer information systems which pose lesser risk thereafter.

Information Security Program

In the Supplemental Information, the Agencies state that a financial institution must adjust the information security plan on a "continuing basis" to account for changes in technology, the sensitivity of customer information and internal or external threats to information security. The Agencies should replace the phrase "continuing basis" with the phrase "periodic basis." Requiring a financial institution to adjust its information security plan on a "continuous basis" is simply unnecessary to account properly for changes in technology and would impose substantial burdens on financial institutions. Instead, the Guidelines should provide financial institutions with the flexibility to decide how often this reevaluation should be done (*e.g.*, on an annual or quarterly basis).

Frequency of Board of Directors Involvement

The Agencies appropriately recognize that a financial institution's Board of Directors should be involved in the development of the institution's information security program. Nonetheless, the Guidelines should provide a financial institution with the flexibility to determine the proper level and frequency of involvement of the Board. For example, the Guidelines should not specify a reporting interval in which the institution's management team must report to the Board (*e.g.*, monthly, quarterly or annually). Specifying one reporting interval that would apply to all institutions is inappropriate since the correct reporting interval for each institution will depend on a variety of factors, such as the

sophistication of the financial institution's management team and information security program.

Board of Directors Delegation

The Guidelines should provide a financial institution's Board with the flexibility to determine how best to carry out its duty to be involved in the development of the institution's information security program. For example, the Agencies should make it clear in the Guidelines that a financial institution's Board may delegate to a committee of the Board primary responsibility for involvement in the institution's security programs, rather than have the entire Board actively involved throughout the process.

Security Testing

The Agencies request comment on whether specific types of security tests, such as penetration tests or intrusion detection tests, should be required. The Agencies should not mandate the use of specific security tests, but instead should allow financial institutions the flexibility to decide what types of security tests are needed and appropriate under the circumstances.

Independent Testing

The Guidelines should not require that the tests or review of tests be conducted by persons who are not employees of the financial institution. Requiring a financial institution to hire outside consultants to perform tests or review test results would impose unnecessary costs on financial institutions with no benefit to consumers. A financial institution should have the flexibility to use its own internal resources or those of an affiliate - such as an internal audit division - to perform tests and review test results. In addition, financial institutions should have flexibility under the Guidelines to decide how best to ensure that: (1) the individuals that are conducting the testing are independent of those individuals that are developing or maintaining the security programs; and (2) the individuals that are reviewing the test results are independent of those individuals that are conducting the tests. The Agencies should not attempt at this time to set forth specific measures that a financial institution must follow when it uses its employees or affiliates to conduct testing and review test results.

Thank you for your consideration of these comments.

If you have any questions or need additional information, please contact me at (202) 296-5544.

Sincerely yours,

RE McKew

Robert McKew
Vice President & General Counsel