45433.pdf

(26)

RUSSELL W. SCHRADER
Senior Vice President and
Assistant General Counsel

VISA

August 25, 2000

By Electronic Delivery

Office of the Comptroller of the Currency
Communications Division
250 E Street, S.W.
Third Floor
Washington, D.C. 20219
Attention: Docket No. 00-13

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the
Federal Reserve System
20th and C Streets, N.W.
Washington, D.C. 20551
Attention: Docket No. R-1073

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

Manager, Dissemination Branch
Information Management and
Services Division
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552

Re: Proposed Guidelines to Implement Section 501 Security Standards

Dear Sir or Madam:

This comment letter is submitted on behalf of Visa U.S.A. Inc. ("Visa") in response to the proposed Guidelines issued by the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision (collectively, the "Agencies") to implement Section 501 of the Gramm-Leach-Bliley Act ("GLB Act"). We appreciate the opportunity to comment on this important matter. In doing so, Visa provides comment generally on the proposed Guidelines, as well as on several specific provisions.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system in the United States and in the world, with more volume than all other major payment cards combined. Visa is part of a worldwide association of over 21,000 financial institution members that individually offer Visa-brand payment services. In fact, Visa now has over one billion cards circulating worldwide. These Visa-branded cards are held by consumers around the globe, and generate over $1.6 trillion in annual volume worldwide and over $700 billion per year in the U.S. At peak volume, Visa's system processes over 3,800 card-related transactions per second. In 1999, the Visa network processed 11 billion credit card transactions worldwide.

VISA U.S.A. INC.
Post Office Box 8999
San Francisco, CA 94128-8999
U.S.A.

Phone 650 432 3111
Fax 650 432 2145

GENERAL COMMENTS ON THE PROPOSED GUIDELINES

As a general matter, Visa commends the Agencies on the approach set forth in the proposed Guidelines. The Agencies appropriately set forth a general framework focusing on the "process" that financial institutions should follow in designing and implementing an information security program, without attempting to specify in detail how a financial institution should structure its information security program. This "general framework" approach provides appropriate guidance to financial institutions, without curtailing the flexibility of financial institutions in developing and implementing an information security program that best fits their particular needs.

FINAL SECURITY STANDARDS SHOULD BE ISSUED AS GUIDELINES

The Agencies issued the proposed security standards in the form of guidelines. In the Supplemental Information, however, the Agencies solicit comment on whether the final security standards should be issued in the form of guidelines or as regulations. The Agencies should issue the final security standards in the form of guidelines, not regulations. The types of administrative, technical and physical safeguards that are appropriate for a financial institution to adopt to protect the security of customer information depend on a variety of factors that vary from financial institution to financial institution -- including the size and complexity of the institution and the nature and scope of its activities. Issuing the security standards as guidelines, instead of regulations, provides financial institutions with the additional flexibility they need to establish an information security program that is appropriate for each individual institution, while also providing institutions with the proper guidance they need to structure their information security programs.

In addition, the Agencies examine financial institutions on a regular basis regarding information security issues, as well as safety and soundness issues. If an Agency, through its examinations of a particular institution, finds that the institution has not adopted adequate safeguards to protect customer information, the Agencies always can impose more specific information security requirements on that institution.

DEFINITIONS

Definition of "Customer"

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, however, 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 information relating to consumer customers. 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. Instead, Congress correctly recognized that businesses are capable of handling their own transactions without additional protection from the government.

In addition, the Agencies should not expand the scope of the Guidelines to cover records regarding all consumers who are not also customers. Limiting the scope of the Guidelines to the records of consumer "customers" is consistent with the plain language of Section 501. Specifically, Section 501 provides, among other things, that the Agencies should adopt appropriate standards for financial institutions relating to administrative, technical and physical safeguards to ensure the security and confidentiality of "customer" records and information.

As the Agencies recognized in the final privacy rules that implement Sections 502 and 503 of the GLB Act, Congress distinguished in the privacy provisions of the GLB Act between "customers" (*i.e.*, those individuals who have an ongoing relationship with a financial institution) and other "consumers" (*i.e.*, those individuals who have obtained a financial good or service from a financial institution for personal, family or household purposes, but who have not established an ongoing relationship). By using the term "customer" in Section 501, 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" -- regardless of whether they have an ongoing relationship -- would expand the requirements of the statute beyond those mandated by the plain language of Section 501.

In addition, because the final privacy rules impose different obligations under Sections 502 and 503 on financial institutions with respect to "customers" and "consumers," some financial institutions may decide it is best to segregate information regarding "customers" from information regarding other "consumers," such as by creating separate databases. Because financial institutions are just now in the early stages of implementing the final privacy rules, institutions may not know at this point whether they will want to ultimately segregate "customer" information from other "consumer" information and whether different security standards are appropriate.

Moreover, even though ultimately many financial institutions are likely to decide to adopt similar security standards for all "consumer" information regardless of whether it is "customer" information, requiring an institution to do so under the Guidelines could expose financial institutions to liability under state laws. Financial institutions that fail to meet the obligations set forth in the Guidelines may be subject to "unfair business practices" claims under state law. Expanding the scope of the Guidelines to apply to all "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.

As a result, the Agencies should continue to specify in the Guidelines that the security standards in the Guidelines only apply to information relating to consumers who are also customers of the institution.

Definition of "Service Provider"

The proposed Guidelines contain a very broad definition of the term "service provider," defining the term to mean any person or entity that maintains or processes customer information on behalf of an institution "or is otherwise granted access to customer information through its provision of services to an institution." The above quoted language should be deleted from the term "service provider." While security standards established by a financial institution undoubtedly will address all who have access to customer information, an entity should not be viewed as a service provider merely because it has such access, particularly given the treatment of service providers elsewhere in the final privacy rules.

Definition of "Customer Information System"

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." This definition of the term "customer information system" is extremely broad. 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. In defining the term "customer information system," the Agencies should focus on the same information systems of financial institutions that are the subject of current examinations.

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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 use of the phrase "continuing basis" in the proposed Guidelines leads to confusion and should be replaced. It is unclear, for example, whether the standard is periodically (*i.e.*, annually or quarterly), or continuously (*i.e.*, someone must be assigned to system upgrades on a continuing basis).

To provide more guidance to financial institutions on this issue, 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 Agencies should make it clear

that a financial institution only is required to reevaluate its information security plan on a "periodic basis." In addition, 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). At a minimum, the Agencies should make it clear that a financial institution is not required to undergo this reevaluation more frequently than on a quarterly basis.

Objectives of an Information Security Program

The proposed Guidelines describe the objectives for an information security program as ensuring the security and confidentiality of customer information, protecting against any anticipated threats or hazards to the security or integrity of such information and protecting against unauthorized access to or use of customer information that could either: (1) result in substantial harm or inconvenience to any customer; or (2) present a safety and soundness risk to the institutions. In the Supplemental Information, the Agencies explain that unauthorized access to or use of customer information does not include access to or use of customer information with the customer's consent. The Agencies should retain this statement in the final Guidelines, and should make it clear that if a customer provides its access device or code (such as PIN or password) to an entity and that entity accesses the customer's information using this access device or code, this access to the customer's information by such entity is not an "unauthorized access to or use of customer information."

DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM

Involvement of the Board of Directors and Management

Under the proposed Guidelines, a financial institution's Board must: (1) approve the institution's written information security policy and program; and (2) oversee efforts to develop, implement and maintain an effective information security program, including the regular review of management reports. The Agencies specifically request comment regarding the appropriate frequency of reports to the Board. The Agencies also ask whether the Guidelines should specify reporting intervals (*e.g.*, monthly, quarterly or annually). In addition, the Agencies request comment on whether the Guidelines should require a financial institution's Board to designate a Corporate Information Security Officer or other responsible individual who would have the authority and responsibility, subject to the Board's approval, of developing and administering the institution's information security program.

In the proposed Guidelines, the Agencies appropriately recognize that a financial institution's Board 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 instance, 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 that vary from financial institution to financial institution -- such as the size, complexity and sophistication of the financial institution's management team.

In addition, 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.

The Agencies also should make it clear in the Guidelines that a financial institution's Board is not required to designate a single Corporate Information Security Officer or other responsible individual who would have the authority and responsibility, subject to the Board's approval, of developing and administering the institution's information security program. Instead, the Agencies should make it clear that a financial institution has the flexibility to determine how best to structure its management team with respect to its information security programs. While many financial institutions may have one person -- such as an Information Security Officer -- who is responsible for developing and administering the institution's information security program, other financial institutions may decide it is best to create a working group or committee for this purpose.

As noted above, the Agencies examine financial institutions on a regular basis regarding information security issues. To the extent that the Agencies find that a particular financial institution has failed to implement an adequate information security program, the Agencies may impose more specific requirements on that financial institution with regard to the structure of its Board's and management team's involvement.

Management and Control Risk

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. The proposed Guidelines also provide 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. 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 final Guidelines to make this clear.

The proposed Guidelines also provide that in establishing a risk management program, a financial institution should consider as part of this program, among other things, 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 final Guidelines that a financial institution is not required to encrypt customer information 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 transmitted and the degree of risk that unauthorized individuals may have access to the data. Under the final Guidelines, a financial institution should be provided the flexibility to decide when it is appropriate to use encryption technology.

The Agencies also request comment on the degree of detail that should be included in the final Guidelines regarding the risk management program, which elements should be specified in the final Guidelines and any other components of a risk management program that should be included. As a general matter, the Agencies should retain in the final Guidelines the level of detail that was used in the proposed Guidelines with respect to the components of a risk management program. The elements specified in the proposed Guidelines are sufficiently specific as to provide appropriate guidance to financial institutions on the elements that should be included in the risk management program, but are not so specific as to curtail a financial institution's flexibility in developing a risk management program that best fits its needs.

Testing of Information Security Systems

In the proposed Guidelines, 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 any 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. The proposed Guidelines also provide that tests shall be conducted, where appropriate, by independent third parties or staff independent of those who develop or maintain the security programs. In addition, under the proposed Guidelines, test results must be reviewed by independent third parties or staff independent of those who conducted the tests.

The Agencies invite comment on the appropriate degree of independence that should be specified in connection with the testing of information security systems and the review of test results. For instance, should the final Guidelines require that the tests or review of tests be conducted by persons who are not employees of the financial institution? If employees may conduct the testing or may review test results, what measures, if any, are appropriate to assure their independence? The final 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 -- such as its internal audit division -- to perform tests and review test results.

In addition, financial institutions should have flexibility under the final Guidelines to decide how best to ensure that: (1) the employees that are conducting the testing are independent of those employees that are developing or maintaining the security programs; and (2) the employees that are reviewing the test results are independent of those employees 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 to conduct testing and review test results.

Overseeing 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 final Guidelines. The Agencies should make it clear in the final 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 should evidence of a violation arise. A financial institution realistically cannot be expected to audit each service provider to ensure that such parties are complying with the final Guidelines, but should be permitted to enforce contractual obligations should violations occur.

In this regard, the Agencies should not set forth specific contract provisions in the final Guidelines 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.

* * *

Again, we appreciate the opportunity to comment on this important subject. If we can assist you further, or if you have any questions regarding the above, please feel free to call at 650/432-3111.

Sincerely,

Russell W. Schrader