

SCHWARTZ & BALLEN
1990 M STREET, N.W. · SUITE 500
Washington, DC 20036-3418
(202) 776-0700

FACSIMILE
(202) 776-0720

M E M O R A N D U M

January 23, 2001

To: Our Clients and Friends

Re: Interagency Guidelines for Safeguarding Customer Information

Summary

The Federal banking agencies have adopted final guidelines establishing standards for safeguarding customer information. The guidelines apply to banking organizations subject to the jurisdiction of the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision. In response to comments, the agencies modified the guidelines in several respects, as indicated below. The guidelines are effective July 1, 2001.

Discussion

Section 501 of the Gramm-Leach-Bliley Act requires the federal banking agencies to adopt guidelines establishing standards for safeguarding customer information. The safeguards are to insure the security and confidentiality of customer records and information, protect against any threats or hazards to the security or integrity of the records, and protect against unauthorized access to or use of the records or information that could result in substantial harm or inconvenience to any customer.

I. Definitions

The definitions adopted by the agencies are essentially unchanged from the proposal.

SCHWARTZ & BALLEN

Customer -- The final guidelines define “customer” in the same manner as the privacy rules adopted by the agencies under §§ 502-510. Accordingly, the guidelines will apply to information about a consumer who has a continuing relationship with the financial institution and where the products or services are used primarily for personal, family or household use. It does not include information about a business.

Customer information – The final guidelines define “customer information” as any record (paper or electronic) containing nonpublic personal information as defined in the agencies’ privacy rules about a customer.

Customer information system – In the final guidelines, this term means any method used to access, collect, store, use, transmit, protect or dispose of customer information. The agencies expanded the scope of this term to include methods of disposing of customer information. As a result, an institution is responsible for safeguarding customer information continues through the disposal process.

Service provider – This term means any person that maintains, processes or has access to customer information through its provision of services to the institution. The term includes only persons who provide services directly to the institution. Accordingly, a subservicer of an institution’s service provider is not a service provider to the institution. However, an institution is required to determine that its service provider has adequate controls to ensure that the subservicer will protect customer information in accordance with the guidelines.

II. Standards for Safeguarding Customer Information

Information security program – Each financial institution is required to implement a comprehensive written information security program appropriate for its size and complexity, and the nature and scope of its activities. The final guidelines clarify that a uniform set of policies is not required for all parts of the organization, although they must be co-ordinated. In addition, the administrative, technical and physical safeguards may be addressed in separate documents rather than in one document. If the program elements are dispersed throughout the organization, they should be capable of being retrieved by management for purposes of co-ordinating and evaluating the program.

Objectives – The final guidelines provide that an information security program is to be designed to ensure the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to such information that could result in substantial harm or inconvenience to any customer. The agencies made two important changes to this provision. First, they provided that the program is to be designed to achieve the above objectives. The proposal suggested that an institution’s

SCHWARTZ & BALLEN

program must achieve the objectives. Second, the agencies removed any reference to protecting against any risk to the safety and soundness of the institution, which was contained in the proposal, because this factor is not mentioned in § 501. The agencies also clarified that “unauthorized access” does not include disclosures made pursuant to an exception contained in the agencies’ privacy rule.

III. Development and Implementation of Information Security Program

The agencies made substantial modifications to this section of the guidelines.

Involve the board of directors – The guidelines continue to require the board (or a board committee) to approve and oversee the development, implementation and maintenance of the institution’s information security program. The board may assign implementation responsibility to a committee or to an individual. If subsidiaries of an institution use the parent’s security program, each board (or committee) must review it to determine if it is suited for that institution. The guidelines clarify that by using the term “oversight,” the agencies meant the board’s conventional supervisory responsibilities rather than some higher level of scrutiny. The guidelines do not require institutions to designate a corporate information security officer.

The guidelines eliminated direct reference to the role of management in implementing and maintaining the program. Rather, the agencies believe that each institution itself should determine to whom such functions should be assigned. Accordingly, the guidelines do not assign specific roles to management.

Assess risk – This provision was revised extensively from the proposal. The proposal required institutions to identify and assess risks that threatened the security of customer information. The guidelines now require the institution to identify “reasonably foreseeable” threats, assess the likelihood and potential damage of these threats, and assess the sufficiency of the institution’s policies and procedures to control risks. The guidelines also permit institutions to determine the levels of protection appropriate for different categories of information.

Manage and control risk – The proposal presented eleven factors that institutions should consider in evaluating the adequacy of policies to manage risk. The final guidelines clarify that a financial institution need not adopt all of the elements presented. For example, encryption may not be appropriate if the institution processes all data internally.

The guidelines provide that an institution must design its information security program to control risks it has identified, consistent with the sensitivity of the information and the complexity and scope of the institution’s activities. The eight factors which should be considered include access controls on customer information

SCHWARTZ & BALLEN

systems, access restrictions at physical locations containing customer information, encryption, dual control procedures, monitoring systems, response programs that specify actions to be taken when unauthorized access has been obtained, measures to protect against destruction, and loss or damage to customer information due to environmental hazards. An institution must consider, but need not adopt, all of these elements as part of its program.

The agencies clarified that by considering appropriate access rights to customer information, they were not intending to confer upon customers the right to access the institution's records. Rather, the factor was intended to refer to possible limitations on the ability of employees to access customer information.

Institutions are also required to train staff to implement the information security program and regularly test key controls, systems and procedures. Tests should be conducted or reviewed by independent third parties or staff independent of those who develop or maintain security programs.

Oversee service provider arrangements – The proposal stated that the institution is responsible for safeguarding customer information even when it gives access to a service provider. The guidelines adopted by the agencies now require institutions to exercise appropriate due diligence in selecting service providers, and require service providers by contract to implement measures designed to meet the guidelines' objectives. Any contract that an institution has with a service provider which is currently in effect is grandfathered until July 1, 2003, even if the contract does not include a requirement that the service provider maintain the security and confidentiality of customer information.

While a service provider need not have a security program that complies with the guidelines, where appropriate, an institution should monitor service providers to ensure that its service providers have met their obligations. Monitoring may take place by means of review audits and summaries of test results.

Adjust the program – Each institution is required to monitor, evaluate and adjust its information security program to reflect changing technology, sensitivity of customer information, threats to information and changing business arrangements.

Report to the Board – Each institution is required to report to its board or board committee at least annually on the overall status of the information security program and on the extent to which the institution's information security program complies with the guidelines.