SCHWARTZ & BALLEN
1990 M STREET, N.W. · SUITE 500
WASHINGTON, DC 20036-3418

(202) 776-0700

FACSIMILE
(202) 776-0720

schwartzandballen.com

M E M O R A N D U M

May 23, 2002

To Our Clients and Friends

Re: FTC Final Rule on
Standards for Safeguarding Customer Information

As required by Section 501 of the Gramm-Leach-Bliley Act, the Federal Trade Commission ("FTC") has issued a final rule establishing standards for handling customer information by financial institutions falling under its jurisdiction.[1] At the beginning of 2001 the Federal banking agencies[2] issued guidelines on the same topic[3] ("Banking Agency Guidelines"). It was the intent of the FTC to issue standards that mirror those contained in these Banking Agency Guidelines. The FTC envisions that any entity that can demonstrate compliance with the Banking Agency Guidelines will also satisfy the requirements of this rule.

The FTC standards are similar to, but more flexible and less specific than the Banking Agency Guidelines. Below is a summary of the major provisions of the FTC rule and its similarities and differences with the Banking Agency Guidelines.

Purpose and Scope

The FTC rule is broader in its application than the Banking Agency Guidelines, as it applies to all customer information in a financial institution's possession regardless of whether such information pertains to individuals with whom an institution has a customer relationship, or pertains to the customers of other financial institutions that have provided such information to the institution.

[1] Institutions included within the FTC's jurisdiction are non-depository institution lenders; consumer reporting agencies; debt collectors; data processors; courier services; retailers that issue credit cards to consumers; personal property or real estate appraisers; check-cashers; mortgage brokers.
[2] Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.
[3] 66 Federal Register 8616 (February 1, 2001).

Definitions

The definitions of "customer," "information security program" and "service provider" are virtually identical to those contained in the Banking Agency Guidelines. To make the definition more appropriate to the entities it supervises, the FTC clarified the definition of "customer information" to include nonpublic personal information handled or maintained by or on behalf of an affiliate of the financial institution. Accordingly, a financial institution subject to the FTC's supervision is required to ensure that affiliates maintain appropriate safeguards if the financial institution shares information with its affiliates.

Standards for Safeguarding Customer Information

Both the FTC rule and the Banking Agency Guidelines require financial institutions to develop and implement a written information security program that is appropriate for their size and complexity and the nature and scope of their activities. For financial institutions subject to the jurisdiction of the FTC, the sensitivity of any customer information at issue must also be taken into consideration.

The objectives of the information security program are identical under the FTC rule and the Banking Agency Guidelines. Both require the program to 1) insure the security and confidentiality of customer information; 2) protect against any anticipated threats or hazards to the security or integrity of such information; and 3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Development and Implementation of An Information Security Program

Oversight. The Banking Agency Guidelines require a board of directors to approve and oversee the development, implementation and maintenance of the institution's information security program. Given the diverse nature of the financial institutions it supervises, the FTC requires a financial institution to designate an employee or employees to coordinate the information security program in lieu of oversight by a board of directors.

Assess risk. Both the FTC rule and the Banking Agency Guidelines require institutions to identify "reasonably foreseeable" risks to the security of customer information and to assess the sufficiency of safeguards in place to control these risks. Unlike the Banking Agency Guidelines, the FTC does not require financial institutions to assess the likelihood and potential damage of threats but does stipulate that risk assessment should include three specific areas of operations: employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and detecting preventing and responding to attacks, intrusions or other system failures.

Manage and Control Risk. Both the FTC rule and the Banking Agency Guidelines require financial institutions to design and implement safeguards to control the risks identified through risk assessment and to regularly test the effectiveness of these safeguards. The FTC rule, however, does not require specific security measures to be considered and does not require testing by independent staff or third parties.

Oversee Service Providers. Both the FTC rule and the Banking Agency Guidelines require financial institutions to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and to require service providers by contract to implement and maintain such safeguards. The FTC requires financial institutions to "take reasonable steps" in selecting such service providers while the Banking Agency Guidelines require that they "exercise appropriate due diligence." The Banking Agency Guidelines describe specific steps financial institutions should take in monitoring the performance of service providers; the FTC rule does not.

Program Evaluation and Adjustment. Both the Banking Agency Guidelines and the FTC rule require financial institutions to continually monitor, evaluate and adjust their information security programs in light of relevant changes in circumstances.

Reporting. The FTC rule does not contain any annual reporting requirements while the Banking Agency Guidelines require an annual report to the institution's board or board committee.

Effective Date

The FTC rule is effective May 23, 2003. Any contract with a service provider that is in effect by June 24, 2002 is grandfathered until May 24, 2004.

The rule can be found at http://www.schwartzandballen.com/WhatsNew.htm.

If you have any questions concerning this request for comment, please call Gilbert Schwartz, Robert Ballen or Tom Fox at (202) 776-0700.