

SCHWARTZ & BALLEN LLP

1990 M STREET, N.W. · SUITE 500
WASHINGTON, DC 20036-3465

(202) 776-0700

FACSIMILE
(202) 776-0720

www.schwartzandballen.com

M E M O R A N D U M

August 25, 2003

To Our Clients and Friends

Re: Proposed Interagency Guidance on Response
Programs to Protect Against Identity Theft

The Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision (the “Agencies”) have requested public comment the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the “Guidance”). The Guidance would apply to all federally-insured depository institutions. Comments are due by October 14.

The Guidance¹ describes the Agencies’ expectations that every financial institution and its service providers must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. A financial institution is expected to develop a response program to protect against risks associated with threats to the security of customer information. The program should include notification to affected customers when a security breach involves “sensitive customer information.”

GUIDANCE COMPONENTS AND NOTIFICATION REQUIREMENTS

The Guidance states that a financial institution’s response program should contain policies and procedures that enable the financial institution to:

¹ In 2001 the Agencies published Interagency Guidelines Establishing Standards for Safeguards for Safeguarding Customer Information (“Security Guidelines”) in accordance with § 501(b) of the Gramm-Leach-Bliley Act, which required the Agencies to establish standards for financial institutions relating to safeguards of customer information and records. See 66 Fed. Reg. 8616 (February 1, 2001). The Guidance interprets the “Security Guidelines.”

SCHWARTZ & BALLEN LLP

- Assess the situation to determine the nature and scope of the incident, and identify the information systems and types of customer information affected;
- Notify the institution's primary federal regulator, and if required, file a Suspicious Activity Report. Where the situation involves federal criminal violations, the institutions should notify appropriate law enforcement agencies;
- Take measures to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- Address and mitigate harm to individual customers through the following corrective measures:
 - Flag and monitor accounts of customers whose information may have been compromised;
 - Secure accounts associated with customer information that have been the subject of unauthorized access or use;
 - Notify affected customers when sensitive customer information about them is the subject of unauthorized access

Notification is required when the financial institution becomes aware of unauthorized access to sensitive customer information, unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur, and takes appropriate steps to safeguard the interests of affected customers, including monitoring affected customer accounts for unusual or suspicious activity. Sensitive customer identification is defined in the Guidance as a customer's social security number, a personal identification number (PIN), password, or account number used in conjunction with a personal identifier (e.g., name, address or telephone number.) Sensitive customer identification also includes any combination of components of customer information that would allow someone to log into or gain access to another person's account, such as a user name or password.

The notification to affected customers should be timely, clear and conspicuous and delivered in a manner that will ensure the customer is likely to receive it. The notice should describe the incident in general terms and the customer's information that was the subject of unauthorized access or use. It should also provide the customer with the following:

- A telephone number to be called for further assistance;
- A reminder to remain vigilant over the next twelve to twenty-four months;

SCHWARTZ & BALLEN LLP

- Inform the customer that the financial institution will assist in correcting or updating information in any consumer report as required by the Fair Credit Reporting Act;
- Recommend that the customer to contact the nationwide credit reporting agencies to place fraud alerts in the customer's consumer reports;
- Recommend that the customer periodically obtain credit reports from such agencies and have any fraudulent transactions deleted;
- Information about the right to obtain a credit report free of charge if the customer believes the credit report contains fraudulent information and about contact information for the credit agencies; and
- Information concerning the availability of the FTC's online identity theft guidance and the FTC web site address and toll-free telephone number from which the guidance may be obtained.

A copy of the Guidance can be found at http://www.schwartzandballen.com/whats_new.html.

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