AMERICAN BANKERS ASSOCIATION

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

October 14, 2003

Filed by email

Public Information Room
Office of the Comptroller of Currency
250 E Street, SW
Washington, DC 20219
Attention: Docket No. 03-18

Ms. Jennifer Johnson
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., NW
Washington, DC 20551
Docket No. OP-1155

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Attention: Comments/OES

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 03-35

Re: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Dear Madame and Messrs:

The American Bankers Association appreciates this opportunity to comment on the proposed Interagency Guidance on Response Programs to Protect against Identity Theft. The proposed guidance is designed to interpret the February 2001 customer information security guidelines issued in conjunction with section 501(b) of the Gramm-Leach-Bliley Act ("existing security guidelines"). According to the notice, the proposed guidelines describe the "Agencies' expectations that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of customer information maintained by the financial institution or its service provider.

The ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country.

Review of the Guidance

The American Bankers Association has been working with our members to assist them with the crafting of information security policies and procedures since the passage of section 501(b) of the Gramm-Leach-Bliley Act. In fact, ABA produced an on-line "member toolbox" on "Safeguarding Customer Information" in 2002 that, among other things, makes it clear that:

> A bank's information security program must be designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that would result in substantial harm or inconvenience to any customer.

The banking industry is thus well aware of the need for strong information security programs and has put in place such programs. It is important that the proposed guidance take this into consideration as it finalizes this document.

The industry also takes its responsibilities to deter identity theft extremely seriously, and has worked with the Federal Trade Commission, the federal bank regulatory agencies, and others to ensure that financial institutions and their customers have the tools available to prevent such thefts and resolve them when they occur. For instance, the ABA has produced an "Identity Theft" communications kit, as well as a "Financial Privacy" toolbox, both of which provide a variety of identity theft prevention and resolution resources.

Overall, while we believe that the agencies have striven to achieve a balance between monitoring accounts and notifying customers, there must be flexibility and discretion afforded financial institutions in determining how to implement this proposed guidance in accordance with individual facts and circumstances. Our comments are directed at areas where clarification is necessary to ensure that flexibility. It should also be noted that implementation of this guidance, in its current form, could result in substantial costs for smaller financial institutions that lack sophisticated monitoring systems.

ABA offers the following specific comments:

- Requirement for Information Security Program
- Risk Assessments and Controls
- Program Requirements
- Service Providers
- Response Program Issues, and
- Customer Notice Issues

Requirement for Information Security Program

In order to remain consistent with the existing security guidelines, we urge the agencies to clarify that the final rules apply only to consumer accounts as is stated in footnote three of the Appendix (Vol. 68 Fed. Reg. at 47958). This becomes important as institutions grapple with the customer notice requirements discussed below.

The proposed guidance tracks the existing security guidelines that, among other things, require every institution to have a security program that protects "against unauthorized access to or use of such information that could result in substantial harm or *inconvenience* to any customer [emphasis added]." Since the proposed guidelines contain more specific obligations, ABA urges the agencies to clarify the term "inconvenience" to the customer so that requirements such as "notice" are not unnecessarily triggered.

Risk Assessments and Controls

We commend the agencies for reiterating that the security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. There is an aspect to the existing security guidelines, however, that ABA recommends be revisited, in that it deviates from a standard of assessing "reasonably foreseeable" internal and external threats.

Under existing security guidelines, financial institutions must adopt specific procedures such as "access controls on customer information systems" and requires that such controls "prevent" an employee from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means. The use of the single term "prevent" is simply too broad and fails to take into consideration that no company or government agency for that matter can monitor every employee's conduct. While banks have long employed various procedures to permit only authorized employees to access customer information, such procedures have technological as well as policy limits. No system is failsafe. ABA urges the agencies to modify the language in existing security guidelines to require controls "aimed at preventing" employees from gaining unauthorized access as opposed to "preventing" such access.

Existing security guidelines also direct that the institution, if appropriate, utilize background checks for certain employees. It should be noted that institutions already fingerprint employees in order to determine whether there has been a previous arrest or conviction but more resources could be made available. Security officers are clamoring for access to data concerning new hires and Congress has even responded with a section in the USA PATRIOT Act on this subject. Section 355 of the Act grants a "safe harbor" to financial institutions that provides written information to another institution concerning a former employee's employment record. To date, we are not hearing that many institutions have taken advantage of this important provision. It would be helpful if the agencies would remind the industry of this background-screening tool.

Service Providers

Third party service providers have a current obligation to protect financial institution customer information against unauthorized access. That obligation exists by contract, based upon the requirement in the existing security guidelines that financial institutions amend their contracts, by July 1, 2003, to require its service providers to implement appropriate security measures. We would recommend that the Agencies specify that financial institutions may place any requirements for reporting security breaches in the contract *or service level agreement* with service providers. Service level agreements are contractually binding. If they are not specified, financial institutions may be under the impression that they must place such language in the overall contract.

Response Program

The Agencies begin this section by stating, in the context of developing a response program, that "internal and external threats to the security of customer information are reasonably foreseeable." ABA believes that not all threats are reasonably foreseeable. Such a statement places an unrealistic expectation on financial institutions and their security programs. We recommend the language be amended as follows:

> The Agencies expect every financial institution to develop a response program to protect against reasonably foreseeable internal and external threats to the security of customer information.

Such language will make it clear that there are instances where a threat is not foreseeable and is consistent with the Administration's overall cyber protection strategy. Many of the threats to the security of customer information are cyber-related. The volume and diversity of these potential threats make it unlikely that any customer information security program will be failsafe. The Administration makes this point in its recently released "National Strategy to Secure Cyberspace," stressing the need for all levels of computer users to "reduce vulnerabilities in the absence of known threats," and further stating that we as a nation "cannot eliminate all vulnerabilities or deter all threats." [1]

The Agencies indicate that every financial institution should develop a *response* [emphasis added] program to protect against the risks associated with these threats, when it is in fact the institution's overall security program that is designed to accomplish this goal. Such language may lead institutions to believe that they must reiterate, in their written response program, much of what is already contained in their existing security program. Language such as "the Agencies expect every financial institution to develop a response program as a part of its overall program to safeguard customer information" would clarify this point.

---

[1] The White House, The National Strategy to Secure Cyberspace, 2003, pp. 7, 27-28.

As threats and vulnerabilities to customer information are not always readily foreseeable, change over time, and vary depending on the characteristics of the financial institution, ABA recommends that the Agencies expressly state that institutions should develop their response programs to be flexible, appropriate for the size of the institution, the risk the institution has based on its technological sophistication, and the products it offers.

For the specifics of the response program, ABA offers the following comments:

- Regulatory Notification

The proposed guidelines suggest that there will be instances when institutions must promptly notify its primary federal regulator when it "becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers." The guidelines also note the requirements under the "Suspicious Activity Reporting"(SAR) regulations on so-called "computer intrusions."[2] There will be much confusion as to what the Agencies are to receive from institutions without clarification. ABA urges that there be no additional notice requirements to the Agencies or customers until there is a detailed analysis as to how an institution must treat the various disclosures. Until these issues are resolved, the final guidelines should make clear that complying with SAR requirements is sufficient and that notification of other regulatory and law enforcement agencies is solely at the discretion of the institution. ABA would be happy to assist in this important effort.

- Corrective measures

Under the proposed guidelines, institutions must take certain measures to "flag accounts." Specifically, the proposal suggests that the institution should "immediately begin identifying and monitoring the accounts of customers whose information may have been accessed or misused."

The ABA recommends that the Agencies clarify that there may be instances where it is advisable for institutions to consider closing the affected accounts. In some cases, after consultation with the customer, it may be better protection for the customer as well as the financial institution to simply close the account, relieving both of the need to monitor the accounts or to respond to endless inquiries. This is especially true for smaller community-based institutions for which it may be more cost effective to close the account for the customer's benefit, rather than monitor it.

---

[2] Computer intrusion (18 USC 1030):
To gain access to a computer system of a financial institution to:
*Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
*Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
*Damage, disable or otherwise affect critical systems of the institution.

The proposal also does not indicate when an institution can cease monitoring accounts. Such monitoring is expensive, particularly for community-based and mid-sized institutions that typically lack the sophisticated automated monitoring tools used by the largest institutions. ABA recommends that the Agencies specify that institutions may cease monitoring accounts when the institution, after appropriate investigation, can reasonably conclude that misuse of information is unlikely to occur and notice is not expected. Doing so would more effectively link the monitoring with the notification process and provide greater clarity to financial institutions as to how the two processes fit together.

Banks are also directed to "implement controls to *prevent* [emphasis added] the unauthorized withdrawal or transfer of funds from customer accounts." As noted earlier, we recommend all references to the charge of "prevention" be modified to reflect the goal of prevention through the use of phrases such as "aimed at preventing." It is impossible to prevent unauthorized transactions in all cases. Transactions may appear to be authorized, but in fact are not. The system simply is not failsafe. Moreover, consumers are protected by various federal laws (Electronic Fund Transfer Act for electronic fund transfers and Truth in Lending Act for credit card transactions) and state laws (Uniform Commercial Code for deposit accounts) for unauthorized transactions.

In addition to identifying and monitoring accounts, the proposal advises institutions to "secure" the account. The meaning of "secure" is not clear. If it means that institutions should stop all transactions, customers could be greatly inconvenienced or harmed. For example, stopping a mortgage payment or payroll payment (if guidelines are applicable to commercial accounts) would harm the customer. Moreover, it would be impractical to obtain the customer's authorization for every transaction. Given that federal and state laws protect consumers against unauthorized transactions, institutions should have discretion on how to manage transactions on the compromised account so as to accommodate customers.

If, on the other hand, "secure" means to close or monitor for unusual activity, it is redundant with the requirement to flag accounts and will cause confusion. For these reasons, we recommend that the final guidelines omit this advice to "secure" the account.

Customer Notice

The ABA recommends that the preamble to the "Examples of When Notice is Not Expected" be amended to specify that financial institutions have the flexibility, after an appropriate investigation *and monitoring of the account,* to conclude that misuse of information is unlikely to occur.

It is also important to note that, in certain cases, the customer may actually be a suspect of the underlying action. Accordingly, the final guidelines should include an exception to the notice requirement if the institution has "reasonable cause to believe that the customer is involved in fraud." This exception, for example, is

presently included in the funds availability schedules under the Expedited Funds Availability Act, which requires that banks make deposits available according to a federal schedule.

In addition, the requirement to notify customers should include an exception if law enforcement notifies the institution that notice to the customer will impede an investigation or enforcement. The guidelines should allow institutions to require that such requests from law enforcement be clear and in writing, to avoid confusion and unfair charges of failure to provide notification.

Conclusion

ABA believes that the development of a customer response program is a valuable component of every institution's customer information security program. We appreciate the opportunity to comment on the proposed guidelines. Such an initiative has sufficient import, in our opinion, that it warrants significant additional discussion and review within the regulatory and financial services community. Many issues have been raised, and we would welcome the opportunity, in whatever forum, to work with the Agencies to further refine the proposed guidelines before they become final. If you have any questions or comments on these matters, please contact Doug Johnson, Senior Policy Analyst at (202) 663-5059.

Sincerely,

James D. McLaughlin
Director, Regulatory and Trust Affairs