



Securities Industry Association

120 Broadway - 35 Fl. • New York, NY 10271-0080 • (212) 608-1500, Fax (212) 968-0703 • www.sia.com, info@sia.com

October 31, 2003

Public Information Room
Office of the Comptroller of the Currency
250 E Street, S.W., Mail stop 1-5
Washington, D.C. 20219
Attention: Docket No. 03-18

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552
Attention: No. 03-35

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the
Federal Reserve System
20th Street and Constitution Ave., N.W.
Washington, D.C. 20551
Docket No. OP-1155

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

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

Ladies and Gentlemen:

The Securities Industry Association ("SIA")¹ submits this letter to the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the "Agencies") on the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the "Guidance").²

¹ The Securities Industry Association, established in 1972 through the merger of the Association of Stock Exchange Firms and the Investment Banker's Association, brings together the shared interests of more than 600 securities firms to accomplish common goals. SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. According to the Bureau of Labor Statistics, the U.S. securities industry employs nearly 800,000 individuals. Industry personnel manage the accounts of nearly 93-million investors directly and indirectly through corporate, thrift, and pension plans. In 2002, the industry generated \$222 billion in domestic revenue and \$356 billion in global revenues. (More information about SIA is available on its home page: www.sia.com)

² 68 FR 47954 (August 12, 2003).

Our members appreciate the opportunity to comment on the Guidance. We recognize that various other trade groups, including the Financial Services Roundtable, have submitted relatively extensive comments that address some of our concerns. Rather than duplicate their efforts, this letter will focus narrowly on our most significant concerns that arise from the Guidance.

I. The Standard for Determining When Notice Must Be Provided to Regulators and Customers Should Be the Same.

In addressing the components of an institution's response program, Appendix Section II. B. of the Guidance discusses when an institution should notify its regulators of an incident. The Guidance requires prompt notification of the primary federal regulator when the institution "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." This is a lower standard than that specified for notice to customers. Appendix Section III provides that institutions should notify affected customers whenever they "become 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...."

Thus, customer notice must occur when a known exposure of customer information likely will result in harm, while notice to regulators is triggered by the mere possibility that harm will result from unauthorized access. We recommend correcting this inconsistency. We believe that the customer notice requirement is the more appropriate standard because it allows the institution to assess the potential injury to its customer, and if injury is unlikely, to avoid the burden of notice provided the institution safeguards customer interests appropriately.

If the regulatory and customer notice provisions are not harmonized, institutions would be required to provide innumerable notices to regulators, which would be burdensome, and overbroad when considered against the goal of the Interagency Guidelines – the protection of customers from fraud and identity theft. For example, when access to sensitive information by an institution's unauthorized employee occurs, the affected institution may reasonably conclude that there is little concern that the employee at issue will misuse the information. With such a broad standard, the proposed regulator notice will likely be of limited use to the Agencies. The Agencies implicitly recognized this in stating that "no useful purpose would be served" by requiring customer notice in response to the "mere possibility of misuse of customer information," as customers need only be alerted to "situations where enhanced vigilance is necessary to protect against fraud or identity theft." 68 Fed. Reg. at 47956.

The customer notice requirement and regulator notice requirements are also inconsistent in the scope of information that is potentially at risk. The customer notice requirement applies to breaches of sensitive customer information, whereas regulator

notice applies to any customer information. In discussing the assessment that institutions are expected to perform regarding likely harm to customers, the Agencies acknowledge that “[s]ubstantial harm or inconvenience is most likely to result from improper access to sensitive customer information because this type of information is easily misused, as in the commission of identity theft.” Appendix Section III. We submit that regulator notice for access to any customer information would be overbroad and unduly burdensome. An unlisted telephone number, for example, may be customer information within the meaning of the Security Guidelines, and unauthorized access to such information might cause the customer inconvenience, but such access would be unlikely to result in fraud or identity theft.

II. The Customer Notice Timeliness Requirement Should Take into Consideration Internal Investigations and Remediation Efforts by Institutions and Potential Notice to Law Enforcement Agencies and Law Enforcement Investigations.

The Guidance is silent on when institutions must provide their affected customers with notice, other than stating in Appendix Section II. D. 3. a. that the notice must be “timely.” In their Request for Comment on Proposed Information Collection the Agencies estimate that that it would take 2.5 business days to develop and produce customer notices and three business days per incident to determine which customers receive the notice and deliver the notices. 68 Fed. Reg. at 47957.

We believe that the estimates by the Agencies may be dramatically unrealistic. The time institutions need to assess any particular incident may exceed such estimates a significant percentage of the time. Determining whether a security breach has occurred will involve investigation of the information systems or operations involved, the potential customer populations affected, and the customer information that may have been accessed. Once response teams determine the severity of the incident, they will need time to assess the appropriate response strategy, including steps to end any malicious activity and restore systems, and/or further collect information to better stop the malicious activity or to press charges against a wrongdoer. Additional steps may be required to limit damage from the incident, including ongoing monitoring, and remedy any security breach.³ The investigation, mitigation and remediation efforts may vary by type of incident or by type of information or technical system implicated. Institutions should therefore be given flexibility to delay any required customer notice until these steps are taken. At a minimum, we believe that the ten business day period recommended by the California Department of Consumer Affairs Office of Privacy Protection in its recent “Recommended Practices on Notification of Security Breach Involving Personal Information,” for compliance with California Civil Code Sections 1798.29 and 1798.82 et seq., should provide institutions with a known safe harbor to complete the steps described above, lest regulated entities be subject to inconsistent notification deadlines for the same incident.

³ We also note that the time needed for such efforts may vary depending on the institution’s portfolio of businesses and the way in which those businesses are supported by technical systems and personnel resources.

Our members also believe that the Guidance fails to consider the effect of potential involvement of law enforcement agencies on the timeliness requirement for delivery of notices. Appendix Section II. B. states that “in situations involving Federal criminal violations requiring immediate attention” the institution should notify appropriate law enforcement authorities. In situations where notice to law enforcement is not required, institutions ordinarily assess the advisability of involving law enforcement on a case by case basis. The factors considered include the scope of the incident and potential harm it raises, the need to be somewhat selective in burdening understaffed law enforcement agencies, the nature of the crime potentially committed, and the ability of the institution to investigate the incident on its own. After a law enforcement agency is contacted, the agency normally takes some time to respond and consider the incident reported, in determining what investigatory and other action it will take. The agency sometimes requests that the suspected incident be kept confidential, or that the institution delay internal investigation and remediation steps, lest any law enforcement investigation or prosecution be jeopardized or hindered. Accordingly, the Guidance should recognize that institutions may delay customer notice when requested by law enforcement authorities, an approach taken by the California legislation referenced above.⁴

III. The Requirement to Secure Accounts Should Allow Institutions Greater Flexibility.

Section II. D. 2. of the Appendix provides that when any account number or other unique identifier has been accessed or misused, the affected account, and all other accounts and services that can be accessed via the same unique identifier must be secured until the institution and its customer “agree on a course of action.”⁵

In light of Appendix footnote 16, which suggests that institutions should also consider changing the account number or the personal identification number, we read “secure” to mean “freeze.” While freezing the account may be one practical solution for an institution that seeks to minimize risk as much as possible, doing so may be detrimental to customers. Pre-arranged payments from such accounts – such as mortgage or other scheduled bill payments – would be stopped by freezing the account. The Guidance should provide that the institution can allow ongoing activity consistent with past customer instructions or otherwise consistent with the history of customer activity in the account, and may otherwise freeze all other account activity as the institution may deem appropriate.

Although the Agencies do not address securities trading accounts, our members’ broker-dealer operations may encounter other operational issues from the securing

⁴ Indeed, if delay to accommodate law enforcement investigatory action is not allowed, institutions would find themselves forced to choose between disobeying a request by law enforcement to delay customer notice, and acting in a manner consistent with the Guidance.

⁵ The disjunctive language in the first portion of the sentence is inconsistent with the conjunctive language in the remainder of the sentence. Where something less than sensitive customer information, as defined, is accessed, we believe that securing the account would be unwarranted because access to the account would not be at risk. Accordingly, we suggest that the Agencies change the language of the sentence by using the defined term.

requirement. Whereas the concern with bank accounts would be the prevention of funds being withdrawn from the accounts, with trading accounts a freeze requirement would require institutions to freeze all securities transactions (e.g., purchases, sales, or both) in addition to withdrawal of funds from the account. In fact, some transactions selected by our customers to mitigate financial risk – such as the purchase or sale of options – might be unnecessarily restricted, with the unintended result of creating more rather than less harm for the customer.

The Agencies specify that accounts be secured until the “customer agrees on a course of action.” We believe that the customer agreement requirement is not appropriate. Institutions often have complex technology infrastructures, and are in a better position than the customer to determine how to protect the particular system affected by an incident, and such steps should not be limited by requiring customer agreement.

Obtaining customer agreement may be particularly impractical when large numbers of customers are involved. Practical difficulties may arise also from the differences between different customer populations. For example, our members may serve high net worth customers, traditional retail customers, or both; these populations often differ in how they receive the institution’s services (electronically through the Internet versus by speaking to an institutional representative), what services they receive, and their level of sophistication about both financial transactions and security risks. We submit that the customer agreement requirement should be eliminated and that institutions be allowed to consider their operations and customer groups in light of their unique characteristics, and to engage in appropriate and situation-specific risk analysis in securing accounts and in lifting the securing steps.

Conclusion

While we laud the Agencies’ efforts on the important customer protection goals of the Guidance, and our members share the commitment to achieving those goals, we ask the Agencies to consider the practical concerns outlined above. We are available to answer any questions the Agencies may have concerning our comments.

Very truly yours,

Scott C. Kursman
Vice President & Associate General Counsel
Securities Industry Association

CC: Aida Plaza Carter, Director, Bank Information Technology Operations Division, OCC
Clifford A. Wilke, Director, Bank Technology Division, OCC
Amy Friend, Assistant Chief Counsel, OCC

Deborah Katz, Senior Attorney, Legislative and Regulatory Activities Division, OCC
Donna L. Parker, Supervisory Financial Analyst, Division of Banking Supervision &
Regulation, Board
Thomas E. Scanlon, Counsel, Legal Division, Board
Joshua H. Kaplan, Attorney, Legal Division, Board
Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision and Consumer
Protection, FDIC
Patricia I. Cashman, Senior Policy Analyst, Division of Supervision and Consumer
Protection, FDIC
Robert A. Patrick, Counsel, Legal Division, FDIC
Robert Engebret, Director, Technology Risk Management, OTS
Lewis C. Angel, Senior Project Manager, Technology Risk Management, OTS
Elizabeth Baltierra, Program Analyst (Compliance), Compliance Policy, OTS
Paul Robin, Special Counsel, Regulations and Legislation Division, OTS