AMERICAN BANKERS ASSOCIATION

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

James D. McLaughlin
Director
Regulatory & Trust Affairs
Phone: 202-555-5555
Fax: 202-828-4548
jmclaugh@aba.com

February 11, 2005

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429-9990

Via E-Mail: IDTheftStudy@FDIC.gov

Re: FDIC report "Financial Institution Letter FIL-132-2004" on December 14, 2004, titled "Putting and End to Account Hijacking Identity Theft"

Ladies and Gentlemen:

The American Bankers Association ("ABA") welcomes the opportunity to offer its comments on this study concerning identity theft. The ABA appreciates the FDIC's efforts to bring better security to online financial transactions and to encourage the growth of online banking and commerce. The ABA would like to commend the FDIC for focusing attention on this growing challenge.

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.

Background

We appreciate the interest of the FDIC and the hard work the Study's authors have devoted to research this issue. As the FDIC knows from its own experience, phishing can be quite detrimental to consumers and institutions alike. The study clearly demonstrates the FDIC's interest in protecting consumers from various forms of on-line fraud and in ensuring that financial institutions continue to serve the financial needs of our customers. The Study, as well as the upcoming Federal Financial Institutions Examination Council symposium on retail authentication being held March 14-25, demonstrates the willingness of the regulatory agencies to have an open discussion with the financial services industry on these issues.

The financial services sector takes identity theft, and indeed any consumer fraud, extremely seriously. In addition to financial losses, the threat to consumer confidence, particularly as it relates to electronic commerce and banking, constitutes a call to action that the industry is rising to in a variety of ways. This view cuts

across the entire industry, as banks of all sizes currently view identity theft as the leading threat against the industry.[1]

Mobilizing against a common foe is not new to the sector. The industry has had great success, for instance, in fighting check fraud over the years. Although the industry's check fraud losses have remained relatively stable since 1999, banks' investment in prevention systems and measures has resulted in an increasing number of fraud attempts being thwarted or caught before any losses were incurred. For example, in 1997, one dollar of check fraud loss was avoided for every dollar actually lost. By 2003, the ratio was seven dollars avoided for every dollar lost.[2]

We are confident that, over time, our industry will have the same measure of success against identity theft. At the same time, we are concerned that some of the rhetoric associated with identity theft, in the media and elsewhere, exacerbates the problem.

Consistent and Accurate Definitions Should be Established

One of our concerns about the study is the terminology used, which we believe will contribute to some of the misconceptions regarding identity theft, account takeover, and unauthorized transactions. In particular, the FDIC introduces yet another term, "account hijacking," into an already crowded lexicon.

In reviewing the study, it appears that it is primarily concerned with unauthorized electronic access to deposit accounts. Yet, the FDIC uses the more vivid and somewhat misleading term "account hijacking." The term is overly-broad, in that it includes, for example, check fraud unrelated to electronic access, which it appears the FDIC is not addressing. The term is also too narrow, in that it appears to be a synonym for "account takeover," because account takeover, as used by the banking industry, excludes single, isolated incidents of unauthorized transactions, which are, in essence, traditional fraud. Rather, "account takeover," as understood and used by the industry, envisions repeated unauthorized access and some level of control, and not, for example, a single, unauthorized use of a debit card by a family member. Like takeover, hijacking assumes control over the account, as opposed to isolated or single incidences.

Banks make these distinctions between account takeover and unauthorized access for the purposes of measuring fraud, developing prevention tools, and resolving consumer disputes. Incorporating an additional term, "account hijacking," for purposes of a study or regulations will be confusing at best, not only for purposes of the study, but when referring to identity theft or account takeover for other purposes. For these reasons, we recommend that the FDIC be precise and refer to "unauthorized electronic access to deposit accounts."

---

[1] In responding to the ABA's *2004 Deposit Account Fraud Survey*, four in 10 bankers ranked ID theft as the number one risk.

[2] American Bankers Association, *2004 Deposit Account Fraud Survey*.

Two-Factor Authentication is One of Many Solutions to Unauthorized Account Access

The FDIC Study contends that unauthorized electronic access to accounts is largely a consequence of (1) reliance on single-factor authentication for customers accessing financial services, and (2) lack of authentication for communications from financial institutions to their customers. While we agree that all institutions must be vigilant, we disagree that reliance on single-factor authentication is largely responsible for the current environment.

While we can all agree that identity theft is a growing problem, it is our view that the traditional criminal methods of obtaining consumer information in the "physical world" – including so-called "dumpster diving" and traditional mail theft, and not phishing, remain the method by which most identity thefts are initiated.

For instance, the 2005 Javelin Strategy & Research Identity Fraud Study found that the most frequently reported sources of information used to commit identity fraud are not computer-based. A lost or stolen wallet, checkbook or credit card was cited by almost 29 percent of the victims who knew how their personal information had been obtained; 11 percent cited friends, acquaintances and relatives; another 8 percent blamed corrupt employees with access to personal information. Computer crimes accounted for less than 12 percent of the perpetrator sources known by victims.[3]

There is a danger in believing that a single deterrence measure, such as two-factor authentication, will in and of itself have a major impact on the level of unauthorized access. Authentication has its place, but at the same time we must use the full variety of resources at our disposal. This includes educating customers and employees on how to avoid the more mundane forms of identity theft that currently lead to a greater number of account takeovers than the ones that occur electronically.

Our own efforts in deploying authentication techniques raise concerns regarding the FDIC's views on the matter. The ABA is an equity participant in Identrus, an identity management company, whose membership consists of more than 55 of the world's leading financial institutions spanning 160 countries. For several years, the ABA, Adobe Systems, Identrus and Wells Fargo have partnered in the creation of SimpleSign™, a product that enables financial institutions of all sizes to create legally binding electronic documents using digital signatures and Adobe PDF files. An Identrus subsidiary, Digital Signature Trust Company is also one of the premier providers of digital identity authentication services to the United States federal government and numerous state governments.

We do not agree, for instance, that two-factor authentication procedures must now be viewed as "industry best practice." Our experience with Identrus, both at the wholesale and retail level, has taught us that customer acceptance is just as important as customer confidence if we are to foster faith in the electronic banking channel. Mandating a best practice does not make it so. Best practices evolve over time.

---

[3] Javelin Strategy and Research, *2005 Identity Fraud Survey Report,* Feburary 2005. Available at: http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html.

We believe that authentication is an important element in a robust information security program; but it is only one element and may not even be the best tool for combating phishing and account takeover. Two-factor authentication methods present both practical problems and complexities. Consumer acceptance, multi-application access, scalability and cost all must be considered when searching for alternative, higher security means. Given the reality that consumers interact with multiple financial institutions, either some means of centralizing token management and authentication needs to be devised or customers would be left with the responsibility of managing numerous tokens for their different financial accounts.

These problems are not insurmountable. In fact, the financial services industry is moving forward with adopting two-factor authentication schemes concurrently with other industries. The Electronic Authentication Partnership, in which the ABA and member financial institutions are active participants, is currently working on standards for interoperability across the public and private sector. The initiative is very promising and should encourage the movement to stronger online authentication.

A Risk-Based, Multi-Faceted Approach is Needed

Under the FFIEC's Guidelines for Safeguarding Customer Information, the agencies have had the foresight to allow institutions, through an appropriate risk assessment, to make their own determinations as to where the risks to their customer information are and what risk mitigation techniques to use. The Guidelines are flexible, risk-based, and technology-neutral. At their core, they are written with the understanding that information technologies, and the vulnerabilities associated with them, are continuously evolving.

We encourage the FDIC to take the same approach to authentication that they have generally taken to information security. The need for information security to evolve as technology evolves points to the value of multiple security layers and controls.

Phishing is really a new way to do what criminals have always tried to do: convincing customers to divulge personal information to a criminal. What stronger mutual authentication will do is give both parties, customers and banks, confidence that an e-mail actually originated from who it says it does. In that way, it can help to prevent phishing. There are other technologies that can accomplish the same thing, and institutions should be allowed to explore them.

Some of the solutions the industry is looking at in conjunction with stronger authentication techniques, include: two-way authentication; certifying e-mails that are coming from a financial institution; addressing malicious code such as key stroke loggers and other forms of spyware; and engaging Internet service providers to block fraudulent e-mail. Financial institutions are working closely with law enforcement to rapidly respond to "phishing" attacks and to shut down the offending servers.

We also urge the FDIC and other FFIEC agencies to join financial institutions to urge software vendors and Internet Service Providers to develop more secure software and platforms with fewer deficiencies and vulnerabilities, requiring fewer

patches. A broad-based program enlisting the Internet Service Providers, law enforcement officials, and others, including building on the consumer education efforts that the financial services sector is already conducting – will provide the most effective response to "phishing," moving beyond an exclusive focus on a technology solution to address the problem in all its dimensions.

The ABA joins FDIC in encouraging all parties involved to strengthen educational programs to help consumers avoid online scams and avoid identity theft, and to take actions to limit consumer liability.

The ABA also encourages all parties to continue to share information with other financial institutions, government agencies and technology providers. The ABA has initiated efforts to share information about online fraud on an international basis. The ABA and many member banks are active participants in the Financial Services Information Sharing and Analysis Center (FSISAC) and encourage greater active participation by all appropriate parties.

Conclusion

The ABA commends FDIC for focusing attention on this growing challenge. We encourage federal agencies to work in partnership with the financial services industry, software vendors and the Internet Server Provider community to promote common standards for establishing identity online and for seeking solutions to make online banking safer for all concerned.

While we do not believe that regulatory action in the form of new regulation or new guidance is needed at this time, we urge the FDIC to work with other FFIEC agencies to adopt uniform supervisory guidance and examination procedures. We also believe it is most important that any actions the financial regulators consider in this area be subjected to the customary process of publication of proposed actions and solicitation of public comment.

We appreciate your consideration of our comments. If you have any further questions or comments on this matter, please do not hesitate to contact Don Rhodes (drhodes@aba.com) or Doug Johnson (djohnson@aba.com).

Sincerely,

James D. McLaughlin
Director, Regulatory and Trust Affairs