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

February 11, 2005

Federal Deposit Insurance Corporation
Ms. Bonnie O'Neill
550 17th Street, N.W., Room 3061
Washington, DC 20429
Attention: **IDTheftStudy@fdic.gov**

Re: FDIC Whitepaper on Identity Theft

Dear Ms. O'Neill:

The Information Security Subcommittee of the Technology Management Committee of the Securities Industry Association ("SIA")[1] appreciates the opportunity to provide comments on the FDIC's recent paper on Identity Theft (the "Paper"). We understand that the Paper is intended to circulate FDIC's findings on unauthorized access to financial institution accounts and how the financial industry and its regulators can mitigate these risks. We hope to add to these findings by sharing the experience of the Securities Industry with respect to identity theft.

We appreciate the FDIC's attempt at clarifying terminology in the "Background" section of the Paper. Identity theft, as defined by the FTC, has many interpretations, and we understand that the FDIC is concerned about three types of activities that are similar sub-activities: credential theft, user impersonation, and fraud.[2] This partition into sub-activities clarifies the fact that, in this form of identity theft, theft is first and foremost of credentials, not money; that stolen credentials are only good when they can be used to impersonate the real account holder; and that fraud is something that may or may not

[1] The Securities Industry Association brings together the shared interests of nearly 600 securities firms to accomplish common goals. SIA's primary mission is to build and maintain public trust and confidence in the securities markets. At its core: Commitment to Clarity, a commitment to openness and understanding as the guiding principles for all interactions between investors and the firms that serve them. SIA members (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. The U.S. securities industry employs 790,600 individuals, and its personnel manage the accounts of nearly 93-million investors directly and indirectly through corporate, thrift, and pension plans. In 2003, the industry generated $213 billion in domestic revenue and an estimated $283 billion in global revenues. (More information about SIA is available at: www.sia.com.)

[2] For a more thorough analysis of the phases with respect to a phishing attack, see the FSTC white paper "Understanding and Countering the Phishing Threat," 2005, available at www.fstc.org.

happen post-theft. It is not literally theft of identity because identity is not taken away from the person; the person still maintains his or her own identity. The person's credentials, once stolen, are only temporarily shared until they can be changed. Theft of credentials may or may not be used for impersonation that results in debt or loss to the person, and when the theft is resolved, the only party suffering financial loss, in many cases, is the Financial Institution because it makes the person whole. We think that the terminology could be more consistently used throughout the paper.

SIA disagrees with many of the stated findings in the Paper. If the findings became prescriptive in the form of ensuing legislation or regulation, this could cause Financial Institutions to redirect effort from their current pursuit of effective methods to combat fraud into ineffective methods. We recommend a more thorough analysis of the issues surrounding the use of the various technologies discussed in the Paper, along with the consideration of additional technologies/tools not discussed. As noted in the Paper, the major challenge lies in identifying the technologies that are acceptable to the consumer while offering the reliability, security, and value required by the Financial Institution. Account hijacking is a complex problem that must be addressed through a range of solutions, both technological and procedural, based on risks, costs, and benefits.

Specific comments that support our overall assessment of the Paper's recommendations are as follows:

Clarity On the Problem To Be solved:

- In the Executive Summary and Findings (page 2), the Paper should acknowledge that issuers/Financial Institutions have already implemented many of the Paper's recommendations. For example, the study indicates Financial Institutions should proactively detect phishing sites; many of our members do so. The study recommends educational programs; these are already in place. Many Financial Institutions have also implemented enhanced detection of phishing fraud behaviors and installed incremental controls. All of these actions however, even when taken together, have not proven to be significantly effective in stopping phishing.
- The Paper focuses disproportionately on the on-line account hijacking problem, even though the statistics presented suggest that this is not as serious a problem as other forms of identity theft, such as identity theft at account opening, identity theft related to check fraud, and identity theft resulting from the insider threat. Additional study should be conducted on these higher risk threats.
- Page 10 implies that fraudsters are hacking into Financial Institutions in order to steal account information. While hackers often target Financial Institutions, the US financial services industry is well guarded against hacking attempts. The hackers, by a wide margin, have much more success attacking customers' personal computers ("PCs") and small businesses' PCs to acquire account information from them than they do hacking into Financial Institution databases.

Need To Balance Customer Acceptance and Risk With Cost and Complexity:

- While two-factor authentication may reduce account fraud, it may not be a cost effective control in all situations. The Paper does not sufficiently qualify the recommendation for two-factor authentication, or recognize that the choice of authentication technologies is not a clear-cut issue.
    - Many of our members recommend or require two-factor authentication (hardware tokens plus a password) for their customers for certain customer activities. Consumer and institutional customers, however, resist such procedures because they are inconvenient or cumbersome, and because if they deal with multiple Financial Institutions they would have the burden of managing several hardware tokens (currently, the technology does not allow a customer to use a single token for accounts at multiple Financial Institutions). Unlike ATM cards, customers cannot simply slip each additional token into their wallets. Moreover, although Financial Institutions routinely provide their customers with secure websites for transacting business in their accounts, customers complain even about the need to log into an institution's website. Although our members strive to protect customers from fraud and to employ effective security methods, we wish to stress that the FDIC and other regulators should weigh a potential two-factor authentication requirement or guideline against customer preferences and the other realities of the marketplace. At the very least, it will take some time to educate and train customers about two-factor authentication methods before they become willing to use them. Mandating two-factor authentication now -- or hailing it as best practice -- would significantly hinder our ability to provide customer friendly online financial services.
    - Customer preferences aside, the use of two-factor techniques for primary authentication may pose undue cost to the Financial Institution and inconvenience to the consumer for low risk activities. In many cases traditional authentication schemes may be sufficient for basic access to on-line services such as customer inquiries or bill payment. Higher value services such as wire- or on-line transfers are better candidates for enhanced authentication methods. Greater attention must be given to the risk of universally applying two-factor authentication over the Internet, using "untrusted" end-user devices, on a scale of tens to hundreds of millions of users.
    - There are usability, maturity, cost and security issues associated with all of the current authentication technology solutions discussed in the Paper, and these need to be considered carefully.

- While the Paper provides an overview of common two-factor authentication techniques, other alternatives should be considered, such as:
    - A secondary authentication code to be transmitted to the user via pre-established channels such as email, phone, or SMS (e.g., a one-time secure transaction code, communicated to the consumer at the time of transaction for certain high value transactions). This technique is also referred to as "out-of-band" communication, as it establishes multiple alerting mechanisms for individuals to identify unauthorized activity with respect to their account.

- Digital certificates to validate a session originating from an authorized customer PC.
- Anomaly detection (detecting customer behaviors or account activity outside of established norms) resulting in account alerts to customers is an effective and low cost method to quickly alert consumers of potential fraudulent activity while allowing rapid response and mitigation by the Financial Institution.
- Additional monitoring techniques to be considered include collection and analysis of PC-specific information such as Internet Protocol address, geographic point of origination, time of day stamps, and other information. This information can be used to detect unusual behaviors that may be related to attempted fraud.
- Restricting access to low risk services and requiring additional registration steps for higher risk/higher value services. This can significantly reduce the population of consumers subject to fraud.

Consideration Of the Landscape Of Threats:

- The Paper does not consider the entire landscape in which identity information may be stolen. For further clarification of this issue, we have included for your perusal an internal SIA discussion document, intended as educational material for legislators.[3] Though some topics discussed in this document were peripherally included in the Paper, we recommend that they be more thoroughly analyzed. For example:
  - Spyware (page 10) should receive greater focus and the discussion should not be limited to the use of key-loggers. Spyware in the form of Browser Helper Objects, Proxies (e.g. Marketscore), etc. are a far bigger threat than presented in the Paper.
  - The last paragraph (page 10) seems to position key-logging as less of a problem than phishing. Our position is that key-logging is the greater threat because key-logging exploits various operating system/browser vulnerabilities and does not rely so much on tricking the victim into replying to a fraudulent request for account information. Customers may be able to spot a phishing email and ignore it, but they will not be aware that a key-logger program is running on their PCs unless their anti-virus and/or spyware software detects it.

Use Of Technology To Mitigate Account Hijacking:

- There is an important technology category missing entirely from the analysis, namely the hardening of customer PCs (this is discussed in some length in the FSTC counter-phishing white paper cited in footnote 2 above). If the user's PC is not cleared of viruses and spyware, then any technology solution that relies on software operating locally on that PC (this includes most biometric reader and USB applications) cannot be trusted to provide a truly secure customer authentication. This implies an

[3] The attached paper is entitled, "Information Security Technology Legislation as seen by a financial industry information security officer." It compares the appropriateness of various authentication technologies to combat various forms of information theft.

important customer responsibility that adds to the complexity and risk of any technology solution, and the technology solution depends upon all customers assuming this responsibility. Specifically:

  - Consumers must assume some level of responsibility for maintaining the integrity of their computing systems.
  - Consumers should be responsible for ensuring their PCs are equipped with updated anti-virus software, personal firewalls, spyware detection, and the latest patches for their browsers and operating systems.
  - This can be conveyed through continued consumer education as well as through technologies to validate the security configuration of the consumer PC.

- An overall weakness of the analysis in this section is reflected in the ratings boxes. They are not only incorrect in many cases, but they are confusing as the technologies discussed address many different aspects of the threat and the effectiveness ratings cannot be easily compared without better understanding which aspect of the threat is being evaluated (see the FSTC's counter phishing white paper's analysis of the phishing life cycle). The Effectiveness rating needs to explain how the rating came about; that is, where the technology is used and how well it works for that purpose. For example, scanning software attempts to stop a phishing attempt in the Set-up Stage of a phishing life cycle through early detection of a fraudulent website. Sender ID attempts to stop a phishing attack during the Collection Stage by identifying a fraudulent email. End-user two-factor authentication attempts to render a phishing attempt useless during the Fraud Stage by making the stolen credentials useless for executing a successful fraud (e.g., attempting a fraudulent account transfer). All of the technology countermeasures discussed are important, but the effectiveness of each measure is tied to the stage of a phishing life cycle threat that it seeks to mitigate, and the several effectiveness ratings cannot be easily compared to each other as if they were substitute technology solutions.
- The ease of use and implementation ratings do not seem to fully consider the complexity, ongoing support, or cost of the proposed solutions, or the trade-off between the risk addressed, ease-of-use, and implementation complexity and cost. This is discussed in more detail below.
- The discussion surrounding email authentication (pages 24-25) is lacking key elements. The Paper makes only minimal discussion of the need for Mutual Authentication – the need for a Financial Institution to authenticate itself to the customer and vice versa. This issue arises when the Financial Institution is sending emails or presenting web pages to the customer. The discussion on pages 24-25 revolves around the use of Sender ID. Sender ID is only one solution, is not the strongest approach, is applicable only for email (but not for web pages), and to date has a mixed record of success. It is at best only moderately effective, and its implementation is difficult because it depends upon email providers/Internet Service Providers ("ISPs") agreeing on a common industry protocol, which is not an easy task.
  - Other technologies in this category include watermarking, digital signatures (e.g., PGP), and presentation of user-specific information or graphics on

emails and web pages to validate the message or web page that originated from the Financial Institution.

- The discussion of shared secrets on page 27 fails to address one-time secrets delivered out-of-band.
- We disagree with the findings on USB tokens presented on page 28. It has been our experience that deployment of USB tokens is not easy. It can require installation of software on a customer PC. Its effectiveness is dependent on a customer properly hardening his or her PC using software that is capable of operating properly on the PC. The conclusion regarding the ease of use of USB tokens also overlooks the customers' need to carry them around. Customers who have relationships with multiple Financial Institutions would need to manage multiple tokens. As we indicate above, we believe customers will continue to resist these requirements.
- The section on smart cards rated the difficulty of implementation of that method as "moderate." It has been our experience that smart card implementation is extremely difficult. There is the significant task of getting a smart card reader installed on the customer's PC as well as the complexity of server-side authentication technology, which normally relies on digital certificate technology. Digital certificates can be compromised just as passwords can, and smart cards can be counterfeited.
- The Password-Generating Token, or OTP technology, discussed on page 29 can indeed be extremely costly when used to support millions of customers. However, it is easier to implement, is portable across devices, and is not more costly than the USB token that was rated "easy" to implement on page 28. As with the USB token, rating OTP tokens easy to use overlooks the multiple financial institution issue, wherein a customer needs to carry multiple tokens.
- We have major concerns regarding the findings on biometric technologies summarized on pages 32-36. It is not clear from our experience with biometrics that any of the biometric technologies justify the ratings of "high effectiveness," "easy to implement," or "easy-to-use."[4] Specifically:
    - Fingerprint recognition technology, which seems to be one of the most mature and successful of the biometrics, is not highly effective or easy to use.
    - The Paper inaccurately describes the accuracy/effectiveness of many of the biometrics discussed. For example, keystroke recognition is portrayed as moderately effective and has the same rating as voice recognition. While we have seen several examples of a successful deployment of voice recognition technology, we have seen no successful deployment of keystroke recognition technology.
    - Our experience indicates consumers do not readily accept solutions that involve lengthy enrollment or require the downloading of files in order to make use of the proposed mitigating technology. In addition, biometric technologies present consumers with well-documented privacy concerns.
    - The section on biometrics lists implementation as "moderate" to implement and "easy" for customers. Yet it also references the difficulties a remote

[4] For further clarification, we attach a paper on biometrics we recently wrote at the request of the Department of the Treasury.

customer would face with enrollment unless the customer had the necessary hardware and software installed on his or her PC. In many cases effective biometrics require in-person registration, which would significantly and negatively impact the ease of use rating. In addition, the cost and implementation of customer-friendly biometric devices is a major undertaking and requires extensive database storage. For example, varying sensitivity calibration could cause customers undue hardship when transactions are rejected because of differences in sensitivity calibration in network equipment.

  - It has been our experience that biometrics are more useful, when used in a well-controlled environment and administered locally to unlock a token, than when they are used to provide remote authentication.

- None of the authentication technologies ratings consider the potential implications of the Americans with Disabilities Act, which may require suitable substitutes for those technologies not accessible by people with disabilities (e.g., the sight- and hearing-disabled and amputees). Currently, Financial Institutions are able to provide substitutes for IDs and passwords.
- Authentication solutions are further complicated by the need to support multiple channels for access to a particular service. For usability reasons, the authentication methods utilized must either be the same or be transparently managed for the customer to address customer acceptance concerns. For example, a password used for online access may also provide access to telephone banking.
- In general, the solutions categorized as "easy to implement" do not take into account critical components of implementation such as cost, overall effectiveness and on-going support, such as accommodating lost, stolen or failed devices and software, or revoking authentication privileges.
- The Paper does not discuss issues with respect to how the two factors are combined to authenticate a user. For example, if the customer cannot be authenticated unless both factors are required to pass, then the likelihood of rejecting genuine customers increases;. If both factors are not required, then the likelihood of an imposter being falsely accepted increases.

Roles:

- In addition to the comments above, the findings section should include a discussion of the roles required of non-Financial Institution players such as ISPs, merchants, law enforcement and email providers. They all play a key role in efforts to reduce online fraud.

SIA wishes to emphasize its belief that fraud cannot be entirely eliminated through a single technology solution such as two-factor authentication. We believe that the Paper achieves a different, although just as critical, purpose: an overview of the account hijacking threat and a discussion of potential tools to mitigate the threat.

Finally, even if the FDIC were to issue a non-mandatory "guideline" or "best practice" recommending two-factor authentication, we would still have the concerns set

forth above. First, the imprimatur of the FDIC on a recommendation of questionable efficacy may be adopted by non-banking agency regulators, thus compounding our concerns and perhaps necessitating guideline revisions that would be needed to prevent inappropriate customer and industry reliance on the guideline. Industry expectations must be managed to maximize flexibility and effective operations so that our members can continue to offer the public the best in financial services. Customer expectations must be managed to maintain customers' willingness to continue to migrate to electronic commerce. Second, even a non-mandatory guideline may help establish a legal standard of care for Financial Institutions, a standard of care that may not be valid and that may provide fodder for unfounded litigation claims against Financial Institutions. Experience shows that technology standards and best practices develop over time, after private and other standards organizations have had sufficient time and deployment trials to gauge whether the standards stand the consumer acceptance test and other requirements businesses face in the practical realities of the marketplace. For example, an incremental path to stronger authentication (in conjunction with other technical controls) may be more appropriate than a single leap to two-factor authentication. Absent further analysis, we believe that this evolutionary process would be disrupted and hindered by a two-factor authentication recommendation or requirement at this time.

We have attempted to identify above those areas where specific guidance provided in the Paper presents concerns for our industry. Our members have substantial practical experience concerning the effective implementation and customer acceptance of the proposed technology solutions/tools discussed, and would be delighted to share our detailed experiences with you regarding our concerns. We appreciate the opportunity to comment on the Paper and would be happy to address any questions you may have concerning our views. Please address questions to the undersigned or to Art Trager, Vice President & Managing Director, Technology, SIA, at 212-618-0546 atrager@sia.com. We would also appreciate the opportunity to participate in any future meetings and discussions you may hold on this subject.

Very truly yours,

Jennifer Bayuk, CISA, CISM
Managing Director, IT Security
Bear, Stearns & Co. Inc. and
Chairperson, SIA
Information Security Subcommittee of the
Technology Management Committee

cc: SIA Information Security Subcommittee
SIA Technology Management Committee