Putting an End to Account-Hijacking Identity Theft

Study Supplement

Federal Deposit Insurance Corporation
Division of Supervision and Consumer Protection
Technology Supervision Branch
June 17, 2005

This publication supplements the FDIC's study *Putting an End to Account-Hijacking Identity Theft* published on December 14, 2004.

EXECUTIVE SUMMARY AND FINDINGS

Focus of Supplement

Identity theft in general and account hijacking in particular continue to be significant problems for the financial services industry and consumers. Recent studies indicate that identity theft is evolving in more complicated ways that make it more difficult for consumers to protect themselves. Recent studies also indicate that consumers are concerned about online security and may be receptive to using two-factor authentication if they perceive it as offering improved safety and convenience.

This Supplement discusses seven additional technologies that were not discussed in the Study. These technologies, as well as those considered in the Study, have the potential to substantially reduce the level of account hijacking (and other forms of identity theft) currently being experienced.

Findings

Different financial institutions may choose different solutions, or a variety of solutions, based on the complexity of the institution and the nature and scope of its activities. The FDIC does not intend to propose one solution for all, but the evidence examined here and in the Study indicates that more can and should be done to protect the security and confidentiality of sensitive customer information in order to prevent account hijacking.

Thus, the FDIC presents the following updated findings:

1. The information security risk assessment that financial institutions are currently required to perform should include an analysis to determine (a) whether the institution needs to implement more secure customer authentication methods and, if it does, (b) what method or methods make most sense in view of the nature of the institution's business and customer base.
2. If an institution offers retail customers remote access to Internet banking or any similar product that allows access to sensitive customer information, the institution has a responsibility to secure that delivery channel. More specifically, the widespread use of user ID and password for remote authentication should be supplemented with a reliable form of multifactor authentication or other layered security so that the security and confidentiality of customer accounts and sensitive customer information are adequately protected.

TABLE OF CONTENTS

INTRODUCTION

The study by the Federal Deposit Insurance Corporation (FDIC or Corporation) called *Putting an End to Account-Hijacking Identity Theft* (Study) was published on December 14, 2004. Public comments were accepted until February 18, 2005. The FDIC is now publishing this Supplement to the Study (Supplement) to

1. Review and respond to the public comments
2. Further survey the most recent trends in identity theft generally and account hijacking in particular
3. Discuss authentication technologies that were not discussed in the Study
4. Present updated findings.

PART 1: PUBLIC COMMENTS AND THE FDIC'S RESPONSE TO THEM

Summary of Public Comments

The FDIC received a total of 70 comments on the Study: 10 from financial institutions, 8 from financial institution trade associations, 32 from technology providers, 9 from independent consultants, 2 from electronic payment system providers, 2 from other types of associations, 6 from individuals, and 1 from a consumer organization. The comments made many useful suggestions that the FDIC has taken into account in this Supplement.

Financial Institutions

The FDIC received comments from ten insured depository institutions, mostly in the small to medium asset size range. Although the comments varied considerably, there were some common themes. Five comments noted that additional consumer education is an effective way to combat identity theft in general and account hijacking by means of phishing in particular. Three comments expressed the opinion that mutual e-mail authentication has the potential to eliminate phishing, and two noted that more secure software, particularly computer operating systems, is necessary to help mitigate the risk of phishing.

Two comments agreed with the FDIC's position that concerns about phishing may slow the growth of online banking. One of those comments went further to add that the Corporation's findings are not strong enough and that section 501(b) of the Gramm-Leach-Bliley Act should be amended to require the use of better authentication technologies. That same comment expressed the opinion that software solutions are, by their very nature, insecure and should not be relied upon.

Three comments disagreed generally with many of the ratings the FDIC assigned to certain technologies. Specifically, three other comments disagreed among themselves about the effectiveness of the scanning software discussed, with two of the comments asserting that such software is available and effective, and one stating that it is not effective as a technique for mitigating account hijacking due to phishing.

Lastly, two comments noted that any action taken by regulators should allow the industry flexibility in implementing a solution, and one of those comments expressed the opinion that the adoption of two-factor authentication will decrease consumers' use of online banking. Three comments took the position that any form of two-factor authentication involving the use or installation of hardware by the consumer will be too costly and will meet with considerable consumer resistance. One comment asked the FDIC to permit additional comment on any proposed guidance before it is issued.

Financial Institution Trade Associations

Of the eight financial institution trade associations that submitted comments, the majority opposed any sort of regulation or guidance in this area, holding that regulation or guidance would be premature. Six of the comments expressed concern that the FDIC may mandate the use of a specific technology by insured depository institutions, and argued that a more flexible, risk-based approach will be preferable. Two comments pointed out that the use of a technology such as two-factor authentication to mitigate account hijacking should be part of a layered approach to information security.[1] However, one association stated that the industry may benefit from the issuance of some form of nonmandatory guidance or best practices.

One-half of the associations objected to the FDIC's use of the term "account hijacking" as too highly charged or inaccurate or both. These comments suggested that the FDIC use the term "account takeover," "account fraud," or "unauthorized electronic access."

With regard to the FDIC's first finding--supporting the use of two-factor authentication--six of the associations took the position that two-factor authentication is not a "panacea" for preventing account hijacking and that many of the technologies discussed in the Study are not mature enough to be extensively deployed. In addition, seven of the associations expressed concern that consumers will resist the introduction of two-factor authentication techniques that involve installing hardware, software, or both on the consumers' PCs. Similarly, four of the associations were of the opinion that a cost-benefit analysis will not support the implementation of two-factor authentication in an effort to mitigate the problem of account hijacking. Two associations criticized the FDIC for not discussing the cost of these technologies in the Study. Three of the associations said the rating charts included in the final section of the Study are not helpful and may even be misleading.

With regard to the FDIC's second finding--supporting the use of scanning software to identify and defend against phishing attacks--two comments noted that such software has been found to be effective and that some financial institutions are already using it. However, one comment noted that such software is not effective.

Five comments urged the FDIC to examine other security techniques that are not discussed in the Study. For example, four comments stressed the importance of mutual authentication as a method of mitigating account hijacking in particular and identity theft in general, and one

[1] Layered security generally refers to the use of a variety of security technologies of differing types to better protect a system.

suggested several specific authentication techniques that the FDIC should investigate, such as out-of-band authentication and device authentication.

Technology Providers

The largest group of comments—32—was submitted by technology providers (TPs), companies that develop and sell computer security products. Eleven TP comments were supportive of the FDIC's Study and findings. However, 3 other comments disagreed with some of the ratings assigned to certain technologies in the final section of the Study. Three other comments stated that the FDIC should avoid prescriptive, one-size-fits-all solutions to the problem.

The comments disagreed among themselves about the effectiveness of consumer education and scanning software. Although three comments expressed the opinion that further consumer education will help to mitigate account hijacking, one comment took the position that consumer education is not effective. Two comments rated scanning software effective in combating account hijacking, whereas one comment stated that such technology is not effective. One comment suggested that the implementation of mutual authentication would be very effective in mitigating the risk of account hijacking. One comment pointed out that, contrary to a statement in the Study, hardware tokens do not always have to be physically connected to a PC.

Most of the TP comments (as well as comments from some of the other groups) discussed seven classes or types of authentication technologies that are not included in the Study. These technologies are listed here and discussed in some detail in Part 3 of this Supplement:

- Internet Protocol Address (IPA) location/geo-location
- Mutual authentication
- Device authentication
- Non-hardware-based one-time passwords/scratch cards
- Trusted Platform Module (TPM) chip
- User-based software to detect phishing and fraudulent Web sites
- Out-of-band authentication.

Independent Consultants

The nine comments received from independent consultants are quite varied. For example, two suggested that the industry and government should focus much more than they do on shutting down phishing Web sites as a way to reduce the incidence of identity theft. Two others stressed the need for mutual authentication so that consumers will know that the financial institution Web sites they are visiting are legitimate.

One comment expressed the opinion that biometric technologies and hardware tokens are impractical for consumer use. That same comment suggested that software tokens are arguably just as effective as hardware tokens and may be more practical to implement as a method for two-factor authentication. This comment also stressed the importance of layered authentication techniques.

One comment took the position that identity theft can be mitigated if "credit freezes" are instituted—that is, if access to credit reports requires the consumer's explicit approval. Since lenders usually refer to credit reports before issuing new credit cards or extending loans, consumers will be alerted to the potential for certain forms of identity theft before the identity theft happens. However, this strategy does not appear to mitigate the risk of account hijacking.

Lastly, one comment noted that a newly released survey indicated that identity theft is no longer the fastest-growing crime and that the proliferation of electronic commerce is not the primary cause of identity theft.

Electronic Payment System Providers

The FDIC received comments from two electronic payment system providers. Both of them urged the FDIC to implement a flexible, nonprescriptive approach to mitigating account hijacking. One comment took the position that the use of two-factor authentication will meet with considerable consumer resistance, that consumer education is important, and that both types of scanning software discussed in the FDIC Study are effective and useful. The other comment disagreed with some of the FDIC's ratings and stated that the Study should have discussed the cost of the various technologies.

Other Associations

The FDIC received comments from two nonprofit associations. Although both were supportive of the Study and the finding supporting the use of two-factor authentication, one took the position that two-factor authentication technologies are ready for deployment, whereas the other said such deployment may be premature. Both comments supported the findings concerning the use of scanning software, consumer education, and information sharing. One comment took the position that mutual authentication is a valuable technique in mitigating phishing attacks.

Individuals

The six comments from consumers were quite varied. Two of them strongly urged government authorities in general to increase the prosecution of identity thieves and impose more substantial sentences. One supported the importance of mutual authentication and the use of USB tokens as the more practical way to implement two-factor authentication. One stated that regulators need to curb access to sensitive personal information via the Internet and supported the value of consumer education. One disagreed with the FDIC's ratings of several technologies.

Consumer Organizations

The FDIC received one comment from a national consumer organization. The comment was supportive of the Study but expressed the opinion that it does not adequately address privacy concerns raised by the use of authentication technologies, particularly the privacy implications of biometrics and e-mail authentication. This comment recommended that the FDIC focus on "smart authentication," that is, authentication technologies that are the least privacy-intrusive inasmuch as they are used for the limited purpose of authenticating the parties in a particular

transaction. The comment supported the use of scanning software and consumer education as ways to effectively combat account hijacking.

The FDIC's Response to the Comments

Terminology

The proper and accurate use of terminology is important for understanding and communicating about identity theft. Many financial institution trade associations took issue with the FDIC's use of the term "account hijacking" as being inaccurate and too highly charged. The FDIC has determined that a variety of terms are used interchangeably to describe this particular form of identity theft. It is the FDIC's view that the term account hijacking is neither inaccurate nor highly charged. Accordingly, the Supplement will continue to use the term account hijacking.

Additional Technologies

Many comments stated that the Study does not discuss a variety of technologies that can be used to make remote customer access to online banking systems more secure. The FDIC agrees, and one purpose of this Supplement is to examine technologies that the FDIC did not consider in the Study (see Part 3 below).

Technology Ratings

A significant number of comments disagreed with the FDIC's ratings of particular technologies. In certain cases, however, comments contradicted one another in their ratings of one or another technology. The FDIC understands from the comments that the technology ratings included in the Study are not helpful to readers and may have fostered more confusion. Ratings have therefore been omitted from this Supplement.

Consumer Education

A substantial percentage of comments agreed with the FDIC's finding that consumer education is an effective way to mitigate the risks of account hijacking. Therefore, commencing in the second quarter of 2005 the FDIC is hosting three public symposia on identity theft; the locations are Atlanta (May 13), Los Angeles (June 17), and Chicago (September 22). During the same period the FDIC will consider conducting consumer focus groups on identity theft.

Earlier in 2005, two other symposia were held. One, on identity theft, was sponsored by the FDIC; it was conducted on February 11 in Washington, D.C. The other, on consumer authentication in an Internet environment, was sponsored by the Federal Financial Institutions Examination Council (FFIEC) and was conducted on March 14–25, also in Washington.

The half-day FDIC symposium consisted of a regulatory/government panel, a financial services industry panel, and a consumer panel, in addition to a keynote address and a wrap-up analysis. The consumer panel, in particular, underscored the rapid rise in identity theft over the past several years, consumers' increasing concerns about this fraud, and the ways in which identity

theft affects consumers' conduct in the marketplace. Industry representatives described their efforts to stop identity theft and, more specifically, the ways in which two-factor authentication is being used to mitigate this risk. A pilot program involving the use of one-time password-generating hardware tokens was said to have been extremely successful in terms of customer acceptance.

The FFIEC symposium, too, examined the problem of identity theft and account hijacking. Industry representatives made presentations to representatives from the federal banking agencies, describing how phishing and other schemes are being used in increasingly complex ways to commit identity theft. Industry representatives also described their successful efforts to use stronger authentication techniques to mitigate this risk.

Two-Factor Authentication as a Panacea

Many comments stated that two-factor authentication—a term that can encompass a wide variety of specific technologies—should not be considered a panacea for the problem of account hijacking and that a one-size-fits-all solution will not work. The FDIC agrees. The Study suggested that two-factor authentication will reduce the risk of account hijacking, not that it will solve the account-hijacking problem; nor did the Study suggest that two-factor authentication cannot be circumvented in certain circumstances. The FDIC Study stated only that two-factor authentication can have a substantial positive effect in reducing the incidence of account hijacking.

Man-in-the-Middle Attacks

Several comments the FDIC received call attention to the fact that certain authentication technologies, including some reviewed in the Study, may be vulnerable to Man-in-the-Middle (MiM) attacks. But most of the ID theft and fraud addressed in the Study and in this Supplement is not perpetrated by fraudsters using MiM schemes. Due to the dynamic threat environment, it is unlikely that any single authentication technology will remain completely immune to all forms of compromise.

Creating a successful MiM attack in a 128-bit Secure Socket Layer (SSL) encrypted session—the kind of session that is typical in Internet banking—is at best, very difficult. In typical Internet-based fraud schemes, the victim's credentials are first collected using automated systems, and then used at a later time to access the victim's accounts. In the collection stage of the attack, fraudsters steal users' credentials by using malicious software such as keystroke loggers or other trojans; sending users to an illegitimate collection Web site using phishing e-mails or pharming techniques; or attacking the communication link using proxy servers or other MiM methods. The account access stage usually requires manual examination of the account. While MiM attacks can easily collect victim's credentials, using the credentials in an automated fashion to access the victim's account is difficult. Accessing the victim's account in real-time is even more difficult to engineer. The divide between data collection and account access stages means that authentication that uses non-collectable methods (token, one-time-passwords, client certificate, etc.) is an effective means for reducing fraudulent account access.

In the FDIC's view, it may be unreasonable to reject an authentication technology because it is vulnerable to a particular attack that accounts for a small percentage of the fraud being perpetrated. The basis for an effective risk-assessment program and information security policy is to implement a comprehensive, layered solution whose pieces deal collectively with the variety of potential threats.

Guidance That Is Flexible and Risk Based

In the press release and financial institution letter (FIL) that accompanied publication of the Study, the FDIC stated that it is considering issuing guidance on this topic later in the year. The FDIC is still considering this option and is in the process of consulting with the other federal banking regulators. However, the Corporation's intention is that any guidance issued will be flexible and risk based, consistent with the Interagency Guidelines Establishing Standards for Information Security (12 CFR part 364, Appendix B).

Public Comment on Future Guidance

A number of comments made the point that any proposed guidance should be published for public comment before being issued in final form. It is premature for the Corporation to commit to publishing for public comment any guidance that may be issued in the future.

Consumer Resistance to Two-Factor Authentication and Possible Adverse Consequences

Many comments, primarily from financial institutions and their trade associations, asserted that consumers will resist the implementation of two-factor authentication and that such a requirement can slow the growth of online banking. While financial institutions must be concerned about losing customers, none of the comments that advanced this argument cited any survey or study supporting that position. Although consumers are certainly interested in convenience, they are also very concerned about the security of their accounts and sensitive personal information. As discussed in the next part of this Supplement, there is evidence that consumers are expecting financial institutions to address the problem of account hijacking and that they will feel more comfortable banking online if they are provided with additional security measures such as two-factor authentication. Several of the seven technologies discussed in Part 3 of this Supplement are more transparent to the customer than the solutions discussed in the Study.

PART 2. MORE-RECENT TRENDS IN IDENTITY THEFT

As the attention paid to the problem of identity theft has grown, additional analyses have been published that shed more light on the size of the problem, the manner in which identity theft is perpetrated, indirect costs, the reactions of banks, the adoption rates and consumer acceptance of various methods of authentication, and public deployment of two-factor authentication.

Size of the Problem

Identity theft is a continuing problem. A recent 2005 study estimates that 1.15 percent of the U.S. adult population experienced a misuse of existing non-credit card accounts or account numbers in the last year, estimates which would include deposit accounts, and another 2.36 percent experienced different forms of identity theft.[2] The Federal Trade Commission reports a slight increase in 2004 in the percentage of bank fraud complaints associated with existing-account fraud and a solid increase in the percentage of complaints involving electronic fund transfers (see table 1). Between 2002 and 2004, the percentage of complaints about electronic fund transfers more than doubled. In addition, for all Internet-related fraud complaints received in 2004, 19 percent of cases in which the complainant reported the method of payment involved a bank account debit, and 13 percent involved a wire transfer.[3]

Table 1. How Victims' Information Is Misused

	2002		2003		2004	
Bank Fraud*	Percentage	Number of Complaints	Percentage	Number of Complaints	Percentage	Number of Complaints
Existing Accounts	8.1		8.3		8.5	
Electronic Fund Transfers	3.1		4.8		6.6	
New Accounts	3.7		3.8		3.6	
Unspecified	2.0		0.5		0.1	
Total Bank Fraud	16.0		17.0		18.0	
Total number of complaints		161,896		215,093		246,570

*Bank fraud includes fraud involving checking and savings accounts and electronic fund transfers.

Source: FTC (2005) p. 10.

The FDIC Study noted phishing as a primary means by which account hijacking is perpetrated. Although some observers are reporting that the number of phishing cases continues to increase

[2] Javelin (2005). The Javelin study attempts to replicate many aspects of the 2003 Federal Trade Commission report cited in the Study. However, differences in methodology preclude longitudinal comparisons of incidence rates. Both studies attempt to measure the following three forms of identity theft fraud: new account and other fraud, misuse of existing non-credit card account or account number fraud, and misuse of existing credit card or credit card number fraud.

[3] FTC (2005). Internet-related is defined as a fraud that concerns an Internet product or service, the company initially contacts the consumer via the Internet, or the consumer responds via the Internet. For Internet-related fraud, 15 percent of complainants reported the method of payment.

and note that response rates to phishing e-mails are consistent with those reported in the Study;[4] other observers are now estimating that phishing is directed at smaller institutions, with response rates at between 1 and 2 percent and declining over time.[5]

Manner of Perpetration

Understanding exactly how identity theft is perpetrated can help regulators, institutions, and consumers identify ways to stop this form of fraud. All identity theft begins with a security compromise of confidential personal data, but linking the security compromise of personal data with the identity theft perpetrator and/or the perpetrator's means of access is difficult and often impossible. These crimes are often unreported and not prosecuted, and they often cross geographic and legal jurisdictions. Victims are unlikely to know that third parties or insiders have stolen their confidential information, or unlikely to be aware that computer spyware, a virus, a hacker, or even phishing is the direct cause of their problem.[6] The more technologically challenging the case, the less likely it is that the victim will understand the means of access.

Two recent studies explore how identity theft is perpetrated. Data from one study do not support the conclusion that "most thieves still obtain personal information through traditional rather than electronic means."[7] As noted above, victims of sophisticated electronic fraud are unlikely to understand how the fraud was perpetrated, so estimates of means of access to confidential information must be interpreted cautiously.

Another study sheds light on a narrow range of identity theft: cases that resulted in arrest or conviction. Although the sample underrepresents the more sophisticated types of electronic fraud as well as crimes that cross legal jurisdictions and all those that are never prosecuted, even for this limited sample it is noteworthy how often the alleged or actual perpetrators acted with others and used the identities of one or more businesses or created bogus businesses to effectuate the fraud.[8]

Indirect Costs

Direct cost estimates of identity theft have been criticized by some researchers as being too high,[9] but the indirect costs are widely considered to be undervalued. Indirect costs include slower adoption rates for online banking and bill paying and therefore a greater use of more-costly banking channels; less effective Internet marketing efforts; loss of consumer confidence in online transactions inside and outside of banking; loss of faith in brand names; and increased concern about financial institution security more generally.[10] Costs resulting from publicity

[4] Department of Homeland Security (2005).
[5] Robertson (2004).
[6] See ibid.
[7] Javelin (2005). Less than half of respondents in the survey reported how they believe the fraudster obtained their personal information.
[8] Collins and Hoffman (2004).
[9] For example, Robertson (2004) and Gould (2004).
[10] See Penn et al. (2005) and RSA Security (2003).

about identity-related security breaches include loss of brand equity, customer defections, lost business opportunities, costly litigation, and the cost of implementing better security.[11]

Measuring the concerns of consumers is one way of understanding the indirect costs of identity theft. Without question, retail consumers are concerned about identity theft and about the misuse of their personal information. Between one-half and three-quarters of U.S. households report that identity theft is a concern for them or that they are concerned about e-mail fraud. Internationally, some 80 percent of online adults worry about their online identity being stolen and used to access online bank accounts.[12]

Although consumers are worried about phishing and the trustworthiness of e-mail messages from their banks, they are also concerned about the security of their personal information more generally. Seventy-five percent of the respondents to one 2004 survey cited identity theft resulting from a security breakdown at the bank as a concern, up from 58 percent in 2003.[13] Consumers who bank online have expressed less confidence in the security of their personal information. When asked the question, 'are you as confident about the protection of your personal information when banking online as when you bank in a branch office,' consumers report a significant decline in confidence (from 74 percent in 2003 compared to 64 percent in 2004). [14] Concerns about fraud are subsumed within retail customers' varying levels of concern about how financial firms handle their personal information,[15] and merchants are concerned as well.[16]

Consumers are indicating that they may stop using or may refuse to adopt online banking because of their security concerns. Online consumers report that they agree with the statements that they will stop using (14 percent) or not enroll (20 percent) in online banking or bill paying because of concerns about phishing. Small business owners' reactions are similar.[17] Security remains a critical factor when a consumer is choosing a retail bank, and one-quarter of international consumers will be very likely to switch banks if, by doing so, they will have better identity protection.[18] One study revealed that two-thirds of respondents said they will switch banks if their bank fails to secure their personal information.[19] A small percentage of consumers—close to 6 percent—have even admitted to having already switched banks to reduce their risk of becoming a victim of identity theft.[20]

Although the costs to banks of consumer concern about security are substantial, the benefits of improved security are likely to be substantial as well. Improved security may open up new

[11] RSA Security (2003).
[12] Louvel (2005), Penn et al. (2005), Graeber et al. (2004), Entrust (2005).
[13] Ponemon Institute cited in Nock (2005).
[14] Ponemon Institute (2005).
[15] See Penn et al. (2005), Graeber et al. (2004), and Entrust (2005).
[16] Almost half of online merchants are more concerned than in the past about online payment fraud, and two-thirds say that a higher incidence of identity theft is increasing the amount of online fraud. See CyberSource Corporation (2005).
[17] Penn at al. (2005). See also Graeber et al. (2004).
[18] Entrust (2005).
[19] Ponemon Institute cited in Nock (2005).
[20] Louvel (2005).

customer markets. Almost three-quarters of current Internet users who do not use online banking report that they will be likely to do so if identity security is improved. Of those that do use online banking, the vast majority report being willing to use more, higher-value services if their identities are better protected.[21] These issues have a far-reaching effect on the business of banking.

The Reactions of Banks

In most cases, financial institutions have a legal responsibility to their online consumers to restore funds (within limits) when they are victims of phishing attacks or of other forms of unauthorized electronic account access. Most banks appear to be taking such responsibility. Some banks appear to be falling short in meeting that responsibility or are making it hard for customer-victims to recover misappropriated account funds.[22] In an attempt to allay consumer concerns about identity theft, some banks have begun advertising a guarantee associated with their online banking. In some cases the wording of the guarantee may be unclear or misleading, and at least one major bank has reportedly been communicating incorrect information to consumers about the bank's security guarantees or the role of the FDIC's deposit insurance in online fraud.[23] Banks should review their procedures for dealing with consumers who become victims of unauthorized access to deposit accounts and should clearly communicate to consumers the precise meaning of any advertised guarantees.

Layered Mitigation Approach

On-line account fraud is usually implemented in various stages and the controls to mitigate the threat can be directed at those stages.

In the first stage, fraudsters must set up their apparatus, including the creation of illegitimate collection Web sites, writing of malicious code, or infiltrating open e-mail proxies. Controls from a financial institution can be directed at detecting the signs of set-up, and preventing (internally) open e-mail proxies. Scanning tools and services can help detect the signs of set-up by reviewing domain registrations and Web site spoofing.

In the second stage, consumers are targeted or fooled into providing their password or other sensitive information with malicious software, misleading e-mail, or illegitimate Web sites. Consumer education is a first line of defense to mitigate this stage. Consumers who understand the risk of installing untrusted software, and who use anti-virus, anti-spyware and firewall controls are less likely to be infected with many of the malicious tools used by criminals. Financial institutions can help by educating their customers about proper computer habits. Additionally, financial institutions can help mitigate the threat at this stage by authenticating their Web sites to differentiate themselves from illegitimate sites. Lastly, the Internet industry is working to reduce the potential of spoofed e-mails through infrastructure changes such as authenticated e-mail. Various services are available to detect and track the dissemination of spoofed e-mails, and other services and techniques can be used to track and take down offending

[21] Entrust (2005).
[22] Penn et al. (2004).
[23] Graeber et al. (2004).

data collection Web sites. Data collection sites and spoofed bank Web sites tend to be short-lived because of these efforts. However, the collected credentials live on to the next stage.

In the last stage, collected credentials are used to access the victim's account. Financial institutions can mitigate this threat with a variety of tools to better identify who is accessing the account. This includes authentication methods which cannot be collected by the fraudster. Financial institutions can also place controls on higher risk account features such as bill payment and account transfers.

Consumer Acceptance of Stronger Authentication

The combination of increased identity theft and intensified focus on preventing terrorism and ensuring business and border security has renewed everyone's interest in methods of authentication. New methods have been developed, and research to create or improve others has been proceeding. Partly because security methods are cloaked in secrecy and partly because the environment has been changing so fast, limited information is available about financial institutions' use of various authentication methods and their effectiveness.

What is known is that within the banking environment, the authentication methods used by corporate banking customers have been stronger and more sophisticated than the methods used by retail customers. The reasons, of course, are the higher account balances—the higher dollar volume of risk—and the more frequent transfer of funds to accounts belonging to third parties. As a result of the authentication methods used, fewer instances of corporate online fraud than of retail online fraud have been reported. A brief look at the authentication methods used by corporate customers may be useful for banks that are considering applying stronger authentication for retail customers.

A small sample of large banks shows that these institutions are using a variety of authentication techniques for corporate banking.[24] Five out of seven global banks and four out of seven North American banks use a single sign-on, with North American respondents generally limiting single sign-on to cash management services. The small sample of large banks uses some combination of user identification, user password, company identification, and company password. Access to trade services, foreign exchange, and investments generally require a separate login and security method for each product.[25] Digital certificates are more often used by large global banks compared to their North American counterparts, primarily to support the nonrepudiation of transactions.

[24] This section relies on Feinberg (2005) which is a supplement to Feinberg (2004). Feinberg (2004) reports on responses of 10 institutions out of 17 large institutions surveyed that are headquartered in North America or with a corporate electronic banking application managed by a North American subsidiary. The 10 respondents were: ABN AMRO, Bank of America, Bank of Montreal, Citibank, Citizens Bank, Mellon Bank, PNC Bank, Royal Bank of Canada, SunTrust, and an unnamed major European bank with a U.S.-managed banking product. Feinberg (2005) discusses the results from those 10 plus 4 more institutions categorized as either global banks (i.e., ABN AMRO, BNP Paribas, Bank of America, Citibank, HSBC, Royal Bank of Scotland, and an unnamed bank headquartered in Europe) or North American banks (Bank of Montreal, Bank of New York, Citizens Bank (a subsidiary of Royal Bank of Scotland), Mellon Bank, PNC Bank, Royal Bank of Canada, and SunTrust).

[25] Feinberg (2004).

Most of these large banks use tokens. Six out of seven North American and global banks included in this sample use tokens to access corporate electronic banking applications, to approve payment transactions, or both. Digital certificates are used by about half the sampled institutions. These large banks have shown little reported interest in using biometrics to authenticate corporate customers.

Online merchants are using, and plan to increase their use of, nonintrusive Internet protocol address filtering methods. Current online merchants are already using a variety of tools, with 33 percent using Internet protocol address filtering and another 22 percent planning to implement that method in 2005.[26]

When banks consider authentication methods for retail customers, they should be aware that these customers value security and the protection of confidential information and may be prepared to use enhanced authentication methods to access their accounts. But there are privacy implications associated with authentication. Consumers report the greatest concerns with biometrics. Consumers will require a clear explanation of any security mechanism and the use of any personal information required to implement that security mechanism. Consumers will need to understand how the additional information will be used and stored. Overly burdensome authentication systems may lower consumer participation, thereby lowering the effectiveness of the entire system. Consumers are also concerned about the risk associated with large databases of personal information and the potential for the information that is used by authentication methods to be compromised, copied, or imitated.[27]

Some conceptual acceptance by consumers of additional authentication methods has been reported concerning biometrics and the willingness of consumers to provide additional information for authentication. Limitations on the use of personal information and the existence of privacy safeguards are important elements of consumer acceptance.[28] Convenience is another element, for convenience plus security may be more important to customers than security alone. In a more recent study, among approximately two-thirds of respondents who found biometrics generally acceptable, voice recognition and finger prints were the most widely accepted biometric types, and convenience was the overwhelming benefit along with security and speeding up the transaction. The one-third who were unsure or opposed to biometrics indicated concerns about how biometrics works and its accuracy.[29]

To an extent, consumers appear to be willing to provide additional pieces of information for authentication (with 29 percent agreeing to provide one additional data item and 41 percent suggesting two).[30] One-fifth of online U.S. households claim that because of their concerns about privacy or security, they would be willing to have an in-home credit card reader.[31] At least

[26] Cybersource (2005). This source uses the term "geo-location" to identify the technology that this Supplement refers to as Internet protocol address location.
[27] National Association of State Chief Information Officers (2004, 2005).
[28] Privacy & American Business (2003).
[29] Magnuson and Reid (2004).
[30] Ibid.
[31] Penn et al. (2005).

one vendor reports interest in two-factor authentication for the accessing of on-line bank accounts.[32]

The challenge facing banks that offer online banking services is significant. New authentication methods must be reliable, cost-effective, and convenient while meeting the security and privacy needs of customers. Cost, reliability, performance, and ease of enrollment are expected to improve in the near term but will still vary by technology and by product within the technology.

Examples of Two-Factor Authentication

At the time the FDIC Study was published, the FDIC knew of several financial institutions that were using two-factor authentication, and contacted them. Each institution asked that its name not be used in the Study. Since then, the FDIC has become aware of additional institutions that have begun using such technologies, and the names of the participating financial institutions have been made public. There may be more institutions becoming interested at least in piloting two-factor authentication programs. A number of institutions have put such programs into production. For two groups, domestic and international financial institutions, tables 2 and 3 list the technology, its application, and the deployment stage as of the date this Supplement was published. Although these tables are not intended to be an exhaustive list of institutions using two-factor authentication, they do suggest that the use of such technology is becoming more common.

[32] Entrust (2005).

Table 2. Domestic Interest in Two-Factor Authentication Programs			
INSTITUTION	**TECHNOLOGY**	**APPLICATION**	**DEPLOYMENT STAGE**
E-Trade Bank	One-time-password hardware token	Internet banking	Pilot
Bank of America	Various two-factor technologies	Internet access for employees and corporate customers	Internal—summer 2005; Corporate customers—fall/winter 2005
Sovereign Bank	One-time-password hardware token	Business banking: corporate and institutional customers	Production
ABN AMRO	One-time-password hardware token	On-line treasury management	Production
ING Direct	Rotating shared secret	Internet banking	Production
Stanford Federal Credit Union	Device authentication	Internet banking	Production
Purdue Employees Federal Credit Union	Biometric (fingerprint)	Automated service centers	Production
San Antonio City Employees Federal Credit Union	Biometric (palm geometry and keystroke)	Safe deposit box access; employee network access	Production
Commerce Bank	One-time-password hardware token	Internet banking for corporate customers	Production
Wachovia	One-time-password hardware token	Internet banking	Under consideration
Dollar Bank	One-time-password hardware token	Internet banking for corporate customers	Production

Table 3. International Interest in Two-Factor Authentication Programs			
INSTITUTION	**TECHNOLOGY**	**APPLICATION**	**DEPLOYMENT STAGE**
Australian Bankers Association*	Various two-factor technologies	Internet Banking	Proposed and pilot programs
Bank of Valletta	One-time-password hardware token	Internet banking, telephone banking, customer service center, mobile banking	Production
Rabobank	One-time-password hardware token	Internet banking	Production
SEB Bank	One-time-password hardware token	Internet banking	Production
SwedBank	One-time-password hardware token	Internet banking	Production
Bank of Tokyo–Mitsubishi	Biometric (palm geometry)	ATM	March 2006
Surugo Bank Shizuoka Prefecture	Biometric (palm geometry)	ATM	Production
Mizuho Bank	Biometric (palm geometry)	ATM	Research
Sumitomo Mitsui Bank	Biometric (palm geometry)	ATM	March 2006
Citibank, UK Division	On-screen virtual keyboard	Internet banking	Production
First National Bank of South Africa	One-time-password hardware token	Internet banking	Production
Royal Bank of Scotland	One time password hardware token	Internet banking	Production
Loyal Bank	One time password hardware token	Internet banking	Production
Fortis, NV	One time password hardware token	Internet banking	Production
Grupo Aval	Device authentication	Internet banking	July 2005
Barclays	On-screen virtual keyboard Out of band	Internet banking Internet banking	Production Under consideration

* According to CEO David Bell, an industry standard requiring all banks in Australia to use two methods of authentication for Internet customers will be introduced in 2005.

PART 3. TECHNOLOGIES TO MITIGATE ACCOUNT HIJACKING

Background

The Study describes three authentication technologies: scanning tools, e-mail authentication, and user authentication. Discussed under scanning tools are the "presumptive forensics" of scanning and server-log analysis software. Discussed under e-mail authentication is the technology commonly referred to as Sender ID. Discussed under user authentication are several techniques for identity management, including shared secrets, tokens, and biometrics.

As noted in Part 1 of this Supplement, however, comments from TPs and others mention several newer technologies that they contend are more transparent to users, and these we describe here. (This is not an exhaustive list of solutions to the problem of account hijacking.) These technologies vary in degree of maturity, vendor base, and level of distribution in the marketplace. Not all of them were commercially available at the time this Supplement was published. For the most part, they are less expensive than the technologies discussed in the Study and are generally installed only on the financial institution's or service provider's system.

The Study includes limited information about the costs of authentication technologies, particularly whether or not the solutions are generally considered expensive to implement and maintain. But given the vast differences in the size and complexity of financial institutions and service providers that will integrate authentication products into their online Internet offerings, it is hard to arrive at meaningful conclusions about specific costs that will apply across the board.

A common measure of the expense involved in enhancing systems is the cost per customer, both to implement the new functionality and to maintain it into the future. A strategy that yields a reasonable cost per customer for a large institution may be considered too expensive for a smaller institution because the larger institution will have more customers over which to spread start-up costs and may benefit from volume purchases.

A major concern in addition to cost is whether the consumer's hardware or software will be affected. Many authentication technologies require the use of hardware and software that must be installed on the host system or on the customer computer, or both. Some technologies require the customer to carry a device for authentication purposes. Among the authentication technologies discussed here are several that can be used with little or no customer involvement. More specifically, for the most part the technologies discussed here require the installation of additional hardware or software only on the financial institution's or service provider's system.

Decisions about which technology to use should be based on research and knowledge acquired through thoughtful and thorough investigation. In particular, the decision to implement more robust authentication techniques should include an analysis of the types of online transactions customers will initiate. For instance, if an online session allows access only to nonconfidential information, a less rigorous authentication technique will be appropriate, for the risk is minimal and it will be impractical to build a complex defense structure to authenticate the session. But if the customer session allows interbank cash transfers, a more sophisticated authentication approach should be used in keeping with the greatly increased risks. Between these two

extremes there are different types of transactions that should be individually addressed, both as to the risks they pose and as to the authentication required by each transaction. Risks and authentication techniques should be commensurate with one another.

Internet Protocol Address (IPA) Location and Geo-Location

What is it and how does it work?

One way to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address (IPA). Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network. If all users were issued a unique IPA that was constantly maintained on an official register, authentication by IPA would simply be a matter of collecting IPAs and cross-referencing them to their owners. However, IPAs are not owned and may change frequently. Additionally, there is no single source for associating an IPA with its current owner, and in some cases matching the two may be impossible.

Some vendors have begun offering software products that constantly scour the Internet for IPA information. These products identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence." The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user's IPA and the profiled characteristics of past sessions match information stored for ID purposes, the user is authenticated. In some instances the software will pick up on out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

In addition to IPA verification, certain geo-location technologies also attempt to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user's location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated. The FDIC is aware of at least one company that markets a commercially available product utilizing geo-location technology.

Capabilities

IPA verification or geo-location may prove beneficial as one factor in a multifactor authentication strategy. However, since geo-location software currently produces usable results only for land-based or wired communications, it may not be suitable for some wireless networks that can also access the Internet—that is, for cellular/digital telephones.

General Requirements

No client software or hardware is required, but integration with existing host applications is necessary since the application resides on the financial institution's or service provider's system.

Customers have no interaction with these software packages and will be unaware of the packages' operation unless informed by their financial institution.

Mutual Authentication

What is it and how does it work?

The Study focused primarily on unilateral authentication strategies when customers are authenticated to the financial institution. However, additional research also showed that many financial institutions do not authenticate their Web sites to the consumer (client browser) before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting consumers cannot tell they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users have trouble telling they are illegitimate. Secure Socket Layer (SSL) coupled with Public Key Infrastructure (PKI) is a widely-accepted scheme for both encrypting and authenticating, with validation capabilities already built into all of the predominant web browser software. When a customer's browser connects to a Web page with an SSL certificate, the browser verifies that the Certificate Authority (CA) that issued the certificate is trusted and whether or not that certificate is still valid. Otherwise, the browser may issue a warning advising the customer that the site may not be secure.

Financial institutions can aid consumers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the client. More specifically, banking Web pages which collect sensitive information on form pages, or otherwise, should authenticate the page using digital certificates signed by a trusted authority prior to collecting the sensitive information. Certificates should be registered to easily identifiable business names rather than third party service providers to aid the consumer's understanding of the certificate's authenticity.

Digitally signed certificates can also be used to authenticate the customer making mutual, or two-way, authentication possible. Certificates issued to a customer can be stored in the customer's browser software, or with special tools, exported to a device. Client certificates can be created by a financial institution and issued to the client for specific use with that institution, or they can be issued by a CA directly to the client and accepted by the financial institution.

For mutual authentication to be performed, valid certificates must be present on the financial institution's Web server and in the customer's browser. Both parties to the session, the financial institution and the customer, may be authenticated through the exchange of certificates.

Capabilities

Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.

General Requirements

Digital certificate technology allowing legitimate Web sites to be authenticated to customers is more expensive than the other technologies discussed in this section. Certificates must be acquired and installed on Web servers as well as on customer systems. Creating policies and a management infrastructure for long-term support must also be considered.

Device Authentication

What is it and how does it work?

Device authentication is a relatively new technology that adds another layer of security by attempting to identify the computer that is being used to access the system or application. The software incorporates technology to examine the unique hardware fingerprint of a PC. This ensures that only a specific authorized device can access a specific online account. Without this specific authorized device, no connection can be made to the network even though the correct password is used. The network is protected since only the authorized device is capable of establishing the connection. However, one disadvantage is that a consumer who attempts to access his or her account while away from home, using a PC that was not previously authorized, will be denied access. If the consumer were to purchase a new PC, that machine would have to be enrolled with the institution before it could be used to access the online banking system.

Capabilities

Device authentication allows only authorized users using previously enrolled devices to enter the network and access the Internet banking application.

General Requirements

Device authentication requires that the software be installed on the financial institution's host system and that each device that will be used to initiate Internet sessions be enrolled with the software. Although no client hardware or software is required, error recovery procedures will be needed to help legitimate users who are unable to access the system.

Non-Hardware-Based One-Time-Password Scratch Card

What is it and how does it work?

Scratch cards are less-expensive, "low-tech" versions of the one-time-password (OTP) generating tokens discussed in the Study. The card, similar to a bingo card or map location look-up, usually contains numbers and letters arranged in a row-and-column format, i.e., a grid. The size of the card determines the number of cells in the grid.

To authenticate, the user will first enter his or her user name and password in the established manner. Assuming that the information is correctly input, as a second authentication factor the user will then be asked to input the characters contained within a randomly chosen cell in the

grid. The user will respond by typing in the grid cell element that corresponds to the challenge coordinates.

Capabilities

Even if a fraudster acquires a user's ID and password, the fraudster will not be able to access the system without physical possession of the scratch card itself. Even if the legitimate user's OTP is compromised, knowledge of that particular OTP will not permit the fraudster to log into the user's account since each login attempt requires the user to input a different OTP from a randomly selected cell on the scratch card.

General Requirements

Conventional OTP hardware tokens rely on electronics that can fail through physical abuse or defects, but placing the grid on a wallet-sized plastic card makes it durable and easy to carry around. This type of authentication requires no training and, if the card is lost, replacement is relatively easy and inexpensive.

Trusted Platform Module (TPM) Chip

What is it and how does it work?

The Trusted Platform Module (TPM) uses an embedded chip to securely store passwords, digital certificates, and encryption keys for PCs. This hardware-based system is designed to verify the authenticity of both the user and the device. The TPM acts as a virtual vault and uses PKI to decrypt, sign, encrypt, and verify both the machine and the application software. The system is designed so that only trusted applications that meet all integrity checks would be permitted. But since all checks and authentications will be performed automatically for the user, the login process will not be expanded or complicated in any way.

Capabilities

The tamper-resistant chip holds keys and certificates associated with the chip and the resident hardware device. The TPM verifies the connected device's integrity at boot-up, and the verification results in a chain of trust between machines. This process protects files from access by unauthorized applications or users. The two most commonly mentioned disadvantages of the TPM are its failure to recognize unlicensed or unrelated software (unrelated to the OS being used) and the cost of converting to another application once a product has been used for any length of time.

General Requirements

Although these chips are being installed on many PCs now distributed by major manufacturers, the chips are disabled. The concept holds promise, but operating system and application support is not wide spread. Plans call for future versions of existing operating systems to begin supporting TPM services.

User-Based Software to Detect Phishing and Fraudulent Web Sites

What is it and how does it work?

E-mail filtering software that attempts to identify potentially harmful e-mail can help consumers recognize fraudulent Web sites, warn them if sensitive personal information is about to be submitted to such a site, and preview Web mail at the server before it is downloaded to the host computer. The use of "disposable" e-mail address software may protect the "real" e-mail account from unwanted and perhaps harmful messages.

The software provides access to a constantly updated database of suspected and known phishing Web sites. Once installed on the consumer's computer, the software monitors the sites on the Internet that the consumer attempts to visit. When a Web site that the software has identified as suspect is selected by the consumer, a warning appears, informing the consumer that the site has been identified as potentially fraudulent. The site can still be visited, but the consumer will be aware of the potential problems related to it. The consumer's computer can be updated automatically or on command, much like most virus protection software packages. The consumer may also click to send a report of a suspected Web site to the software provider's central database. Some filtering software contains a feature that allows the user to preview e-mail. Previewing e-mail enables the consumer to set parameters that will allow only trusted mail to be immediately downloaded and will ensure that suspect mail is either deleted at the server or quarantined if a virus or worm is suspected.

The use of disposable e-mail address software enables the consumer to maintain a private, less accessible e-mail account when enrolling in Internet banking. Use of a separate disposable account for each membership will preclude the dissemination of the consumer's e-mail account and common login information.

Capabilities

Filtering and disposable e-mail software offer consumers a safer way to browse the Internet and use e-mail. The level of protection and effectiveness offered by filtering software depend on the consumer not ignoring the warnings generated by the software when it detects a potentially fraudulent Web site. The use of disposable e-mail addresses may reduce successful phishing attacks by making sure that phishing e-mails are never received by the consumer.

General Requirements

This software is currently available, and several variants of each type of product are freeware. The consumer-based character of this protection allows the consumer to install it on multiple PCs.

Out-of-Band Authentication

What is it and how does it work?

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. In previous versions, a transfer of funds, a purchase, or some other monetary transaction was received by the financial institution from the customer either by telephone or by fax. After the institution received the request, usually a telephone call was made to another party within the company (if a business-generated transaction) or back to the originating individual. The telephoned party was then asked for the predetermined word, phrase, or number to verify that the transaction was legitimate and also to confirm the dollar amount. This layering precluded unauthorized transactions and also caught dollar mistakes, especially when a $1,000.00 order was intended but the decimal point was misplaced and the amount came back as $100,000.00.

In today's environment the methods of origination and authentication are more varied, and the originator may be an Internet banking account holder, an online shopper, or an international customer. The types of call-back are also more adaptable and imaginative. The millions of cellular phones, land-line telephones, PDAs (personal digital assistants), and VoIP (Voice-over IP) telephones provide for both manual and automatic transaction authentication. For example, when a user initiates an online transaction, a computer or network-based server generates a telephone call or an e-mail or text message. When the proper response—a verbal confirmation or an accepted-transaction affirmation—is received, the transaction is consummated.

Capabilities

This type of layered authentication would preclude most man-in-the-middle concerns. However, as with any authentication method, if the authenticating device and/or response were otherwise obtained by criminal elements, the system could be compromised.

General Requirements

Some households still do not have access to high-speed Internet access and must rely on telephone dial-up connections. For such users who also do not have a cellular phone, this system would be harder to use, although the use of e-mail authentication would still be possible. And although cellular phone ownership is sizable and coverage extensive, some areas of the country still have unreliable wireless connectivity.

PART 4. FINDINGS

The FDIC Study generated a considerable amount of interest, discussion, and comment. After reviewing the public comments, further surveying the most recent trends in this area, and researching additional authentication technologies, the FDIC is of the opinion that the findings contained in the Study are sound and supportable.

The Study and Supplement illustrate that identity theft continues to be a growing problem for the industry and consumers. These two publications also show that a wide variety of technologies are available to help mitigate the risk of identity theft. The technologies vary in terms of their maturity, cost, ease of use, and effectiveness. However, many of them have the potential to substantially reduce the level of account hijacking (and other forms of identity theft) currently being experienced. The technologies discussed in this Supplement are for the most part less expensive and more customer friendly than those discussed in the Study and merit consideration as cost-effective ways to address the problem.

Different financial institutions may choose different solutions, or a variety of solutions, based on the complexity of the institution and the nature and scope of its activities. The FDIC does not intend to propose one solution for all, but the evidence examined here and in the Study indicates that more can and should be done to protect the security and confidentiality of sensitive customer information in order to prevent account hijacking.

Thus, the FDIC presents the following updated findings:

1. The information security risk assessment that financial institutions are currently required to perform should include an analysis to determine (a) whether the institution needs to implement more secure customer authentication methods and, if it does, (b) what method or methods make most sense in view of the nature of the institution's business and customer base.
2. If an institution offers retail customers remote access to Internet banking or any similar product that allows access to sensitive customer information, the institution has a responsibility to secure that delivery channel. More specifically, the widespread use of user ID and password for remote authentication should be supplemented with a reliable form of multifactor authentication or other layered security so that the security and confidentiality of customer accounts and sensitive customer information are adequately protected.

REFERENCES

Collins, Judith, and Sandra Hoffman. 2004. Identity Theft: Predator Profiles. Unpublished paper. Michigan State University, School of Criminal Justice.

CyberSource Corporation. 2005. Sixth Annual On-line Fraud Report.

Ensor, Benjamin, Martha Bennett, and Tim Van Tongeren. 2005. Why Banks Must Tackle Net Users' Security Fears. Forrester Research.

Entrust. 2005. Customer Perspectives on Identity Theft and Phishing: Entrust Internet Security Survey.

Federal Trade Commission. 2005. National and State Trends in Fraud and Identity Theft: January–December 2004.

Feinberg, Susan. 2004. Strong Authentication in Corporate Electronic Banking: North American Survey Results. TowerGroup.

———. 2005. Authentication in Corporate Electronic Banking: Are Major Global FSIs Just Making a Token Effort? TowerGroup.

Gould, John. 2004. Retail Financial Fraud: A Seismic Shift. TowerGroup.

Graeber, Catherine, Ron Shevlin, and Adele Sage. 2004. Phishing Concerns Impact Consumer On-line Financial Behavior. Forrester Research.

Javelin Strategy and Research. 2005. 2005 Identity Fraud Survey Report.

Louvel, Sophie. 2005. Document Overview: ID Theft Concerns Change U.S. Consumer Banking Behaviors. Online. Financial Insights. Available at www.financial-insights.com (accessed April 22, 2005).

Magnuson, Gail, and Peter Reid. 2004. White Paper: Privacy and Identity Management Survey. EDS and International Association of Privacy Professionals.

National Association of State Chief Information Officers. 2004. Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications.

———. 2005. Welcome to the Jungle: The State Privacy Implications of Spam, Phishing and Spyware.

Nock, Howard. P. 2005. Fourth District Conditions. Online. Federal Reserve Bank of Cleveland. Available: www.clevelandfed.org (accessed April 27, 2005).

Penn, Jonathan, Bill Doyle, and Adele Sage. 2004. Financial Institutions Are Unwitting Contributors to Identity Theft. Forrester Research.

Penn, Jonathan, Penny Gillespie, Bill Doyle, and Adele Sage. 2005. Keeping Financial Transactions On-line: Stronger and More Visible Security Will Attract Customers. Forrester Research.

Ponemon Institute. 2005. 2004 Privacy Trust Survey for Retail Banking.

Privacy and American Business. 2003. Press Release (January 7): New Survey Shows Public Willing to Accept Biometric Identifiers but Demands Privacy Safeguards.

Robertson, Elizabeth. 2004. A Phish Tale? Moving from Hype to Reality. TowerGroup.

RSA Security. 2003. An Enterprise Perspective on Identity Theft.

Tubin, George. 2005. The Sky IS Falling: The Need for Stronger Consumer On-line Banking Authentication. TowerGroup.

U.S. Department of Homeland Security. 2005. Draft Report of the Phishing Roundtable.

U.S. Department of the Treasury. 2005. The Use of Technology to Combat Identity Theft: Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003.