

STATEMENT OF

**SANDRA L. THOMPSON
DEPUTY DIRECTOR
DIVISION OF SUPERVISION AND CONSUMER PROTECTION
FEDERAL DEPOSIT INSURANCE CORPORATION**

on

“Enhancing Data Security”

before the

**SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT**

of the

**COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES**

May 18, 2005

Thank you Mr. Chairman, Representative Sanders, and Members of the Subcommittee. I appreciate the opportunity to present the views of the Federal Deposit Insurance Corporation on the issue of data security and protecting sensitive information. The FDIC shares the Subcommittee's concerns about the harm to consumers caused by theft of personal financial information.

Since the early 1970's, the FDIC has treated data security as a significant risk area due to its potential to disrupt bank operations, harm consumers, and undermine confidence in the banking system and economy. The failure or misuse of technology can impact the safety and soundness of an institution with sudden and severe losses, or directly harm consumers.

My testimony today will turn first to emerging trends and developing threats the FDIC is seeing in terms of security breaches. I will discuss as well the FDIC's examination programs, including existing regulations and guidance, which require banks to keep their data secure. Finally, I will discuss our outreach efforts to the industry and consumers.

Emerging Trends and Developing Threats

In its role as supervisor, the FDIC analyzes emerging cyber threats, occurrences of bank security breaches and other incidents. Data compromise and misuse are not new issues. Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving. Due to the evolving nature

of threats, the ability to secure customer data against compromise will never be 100 percent assured.

The Internet and other technologies facilitate identity theft by offering a marketplace for the quick sale of confidential information. Not only is the Internet an integral component in nearly every facet of legitimate U.S. commerce, it also has lent its global presence to the sale and ultimate misuse of data to a degree that did not exist previously.

In addition to the Internet's far reaching beneficial attributes, the Internet has created an anonymous and lucrative channel that provides an accessible market for, and adds value to, stolen data. The Internet has made it possible to build a virtual storefront, without geographic boundaries, that criminals can use to conduct business on an increasingly larger scale.

For discussion purposes, it is useful to distinguish between information theft and information fraud. The information theft stage is targeted at consumers through schemes such as phishing, malicious software (i.e. spyware and trojans), or pharming at financial institutions through cyber intrusions from mis-configured systems or other vulnerabilities, the mishandling of data, or by insider abuse of data. Information fraud is generally targeted at financial institutions, merchants, or other servicers in order to extract value out of the information. We will discuss the most common types of attacks that we see on consumers and financial institutions.

Consumer Targeted Attacks

Malicious software on users' computers, phishing schemes, and pharming technologies are all aimed at consumers. Consumer awareness and education can mitigate or reduce some of these threats to personal information security. However, financial institutions and companies that store, transport and use consumers' information also have a responsibility in protecting that data.

Malicious Software - Consumer targeted attacks can include the delivery of spyware, keystroke loggers (programs that track and record a user's keystrokes), trojans, and other malicious code that intercept Internet access credentials (e.g. passwords) in order to commit fraud. Typically, malicious software may be bundled as a hidden component of other programs or inadvertently downloaded from the Internet. Usually, these programs are installed without the users' knowledge. In some cases, the software has even requested that users agree to the activity by including opt-in agreements. The FDIC plans to issue industry guidance advising financial institutions about potential spyware threats later this year.

Phishing - Phishing and spoofing continue to increase and now comprise over 50 percent of the incidents reported to the FDIC. Phishers have begun attacking smaller financial institutions, expanding their operations as the larger often phished banks become less fertile. The FDIC recently published a study, discussed later, that recommends financial institutions and service providers consider stronger risk based authentication strategies to reduce fraud related to compromised Internet account access credentials. An increasingly large number of banks are

introducing stronger authentication strategies for higher risk customers. The Federal Financial Institutions Examination Council (FFIEC) also has plans to release guidance related to authentication later this year.

Pharming - Pharming is a relatively new term to describe the practice of web-site redirection. Fraudsters can hijack, or steal, a company's web site name, or redirect unknowing users to phony web sites where they collect confidential data. Several industries have been attacked using pharming techniques. The FDIC issued guidance to financial institutions related to protecting and securing web site domain names as one method to prevent pharming attacks.

Financial Institution and Merchant Targeted Attacks

Credit Card Data Theft - Credit card data is a valuable commodity for criminals, as evidenced by the recent rash of publicized events. Some merchants store the credit card data collected, at the time of a sale, on their own internal computer systems. In most cases storing customer credit card data in this manner is a violation of card processing agreements. If merchant computer systems have not been adequately secured, hackers are able to connect to the credit card data stored in the vulnerable systems and copy or offload credit card information. In our experience, a compromise such as this is generally not discovered until fraudulent transactions begin to appear in cardholder accounts. Controlling the exposure is dependent upon the time it takes to verify the fraud and discover the source and extent of the compromise.

Patch Management and System Updates - In many cases, systems containing confidential data have not been updated or patched to eliminate vulnerabilities. Operating systems, software applications, Internet browsers, wireless networks, and other communication channels intended to facilitate legitimate business activities are prime targets for illegal entry as new vulnerabilities are discovered. Patches and product updates to remedy these problems are created by manufacturers and third party vendors frequently -- sometimes on a daily basis. Given the complex assortment of products required to conduct business in a largely electronic environment, an effective patch management and update program is essential for maintaining data security. A recent large scale vendor data compromise occurred because its wireless networks were not sufficiently secured. The FDIC has issued guidance to the industry on the importance of maintaining an effective computer patch management program.

Data in Transit - The loss of tapes containing sensitive information while in transport, as reported recently, is not a new threat. However, awareness that such losses can contribute to identity theft is growing. The regulators, as part of their examination process, review bank procedures for transportation and storage of critical and sensitive media. The FFIEC, in its IT Examination Handbook, recommends suggested practices for transporting backup tapes including methods for administrative, physical, and technical controls.

Financial institutions regularly transfer back-up data to secure locations using bonded and licensed courier services. There have been a number of recent instances involving the loss of tapes or other magnetic media, containing confidential customer information, while in transit between the institution and a storage facility. Encrypting data that is being transferred off site

would effectively mitigate this risk of loss but is not widely practiced due to the resources required to encrypt the information as well as the implications created by having to decrypt data as part of the recovery process associated with a primary system failure. Regulatory guidance advises financial institutions to take appropriate measures to ensure the safety of any confidential data that is being moved off site, but does not require encryption.

FDIC Identity Theft Study and FFIEC Guidance

The FDIC's concern with identity theft generally and account hijacking in particular led us to undertake a study to identify causes and possible solutions to this type of fraud. The FDIC published a study, entitled "Putting an End to Account-Hijacking Identity Theft" (Study), on December 14, 2004. The Study presents the FDIC's findings on how fraudsters get access to consumers' bank accounts and how the financial services industry and regulators can improve security to mitigate these risks. A supplement to the study will be published soon. As part of the Study, the FDIC identified several courses of action to help reduce account hijacking identity theft:

- The industry should implement more secure authentication methods for consumers using Internet banking. The current system of user IDs and passwords can easily be thwarted.
- Education programs can help consumers avoid online scams such as phishing. The federal financial regulators have published a "statement stuffer" pamphlet that financial institutions can use to help educate their customers of the risks of disclosing personal information over the Internet and to inform customers of positive computer habits such as

using anti-virus software, firewalls, and regular security updates to their systems. The FDIC also is planning for the future delivery of a consumer oriented education effort to teach consumers how to create a safer computer environment and to avoid on-line scams, such as phishing, that can lead to account hijacking and other forms of identity theft, as well as how to take action to limit liability.

- Encouraging the increased use of new technologies can help financial institutions and consumers to proactively identify and defend against phishing attacks.
- A continuing emphasis on information sharing among the financial services industry, government, and technology providers. The FDIC is hosting several identity theft symposia throughout the country to encourage and facilitate a dialogue with the industry and consumers about this issue and our findings.

As an outgrowth of our Study, the FDIC is leading a FFIEC working group to draft guidance that would set forth the regulators' expectations concerning increased security measures for Internet banking. We anticipate this guidance will be published later this year.

Examination Programs

Even before the explosive growth in the use of technology and the development of the Internet, banks and their regulators have recognized the significant importance of protecting

confidential customer data. Over the years, the entire financial sector has increasingly relied upon technology to implement core business strategies, conduct operations, create efficiencies, secure customer data, control against internal and external fraud, comply with regulations and identify new risks and opportunities. The banking regulators have included data security as a factor in the overall risk assessment of most financial institutions for over 30 years with a focus on ensuring data integrity and business continuity.

The FDIC monitors security issues in the banking industry on a regular basis through on-site examinations, regulatory reports, and news events. The FDIC works with groups such as the Finance and Banking Information Infrastructure Committee (FBIIC), the Antiphishing Working Group, other regulatory agencies, law enforcement and others to share information regarding emerging issues and coordinate our responses. While recent events in the news appear noteworthy, overall our financial institutions have strong controls. The banking regulators monitor over 8,000 financial institutions, all of which transmit or transport data on a daily basis. While a serious problem, the relative number of incidents has been small compared to the volume of transactions. At the same time, we are aware that a single incident can impact thousands of consumers. Therefore, constant vigilance is critical.

To address the specialized nature of technology related supervision, risks, and controls in the banking industry, the FDIC regularly and routinely evaluates all of its regulated financial institutions' information security programs through our information technology (IT) examinations, as well as enforcing legal privacy requirements through our compliance examination program. As mentioned earlier, the FDIC's most direct role in ensuring cyber

security within the financial sector is through its on-site examination programs. The FDIC also conducts IT examinations of major technology service providers that support financial institutions. Through the national examination program, on-site reviews of large technology service providers are conducted on an inter-agency basis.

As you know, Congress has passed several key laws designed to protect personal information. These laws have become part of the business of banking and include the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transaction Act (FACTA), and the Fair Credit Reporting Act (FCRA). The statutes are largely implemented through regulations and interpretations and are enforced by the FDIC and other regulatory agencies through routine on-site examinations of financial institutions. Institutions that fail to comply with these laws may face enforcement actions ranging from informal agreements to civil money penalties or other administrative actions.

The FDIC takes a proactive approach to enforcing data security regulations and guidance. As part of regularly scheduled examinations, our examiners evaluate each financial institution's program for securing customer data. If that program is inadequate, the FDIC takes action regardless of whether or not there has been a compromise in data security. Depending on the severity of the findings, informal or formal enforcement action may be pursued.

For example, in a recent examination, information technology examiners identified an institution with a weak information security program that could have resulted in a breach of customer data. Weaknesses included inadequate risk assessment, inadequate policies, and

inadequate procedures for securing data. The examiners pursued a bank board resolution that included provisions to enhance the bank's risk assessment process, improve administrative controls, verify firewall controls, and develop procedures to address software and system changes, including patch management. The status of the resolution is tracked by the FDIC until each of the items is resolved by the institution. Institutions that fail to resolve problems or implement corrective action recommended by our examiners may be subject to more formal enforcement actions.

In another case, an institution operating under a memorandum of understanding (MOU) for a variety of safety and soundness and information technology issues was not correcting the problems satisfactory. A cease and desist order (Section 8(b) of the FDI Act) was issued and the institution was ordered to establish a specific timetable to conduct periodic penetration and network tests.

In response to Title V of GLBA, the FDIC implemented the *Privacy of Consumer Financial Information* regulation in Part 332 of its regulations. This privacy rule limits disclosure of nonpublic personal information by financial institutions. Subject to certain exceptions, the Privacy Rule prohibits financial institutions from disclosing a consumer's nonpublic personal information to a nonaffiliated third party unless the financial institution satisfies certain notice requirements and the consumer does not elect to prevent, or "opt out of," the disclosure.

FCRA as amended by FACTA in 2003, also contains many requirements dealing with consumer reports, and establishes new rights for identity theft victims. Newly effective requirements in the FACTA include:

- *Fraud and Active Duty Alerts* - Consumers may place alerts on their credit reports when they are victims of identity theft, or if they are members of the armed services who have been called up to active duty. Banks obtaining consumer reports that contain these alerts must take extra steps to identify the consumer to ensure that someone is not, for example, fraudulently applying for credit or opening a new account;
- *Disclosures of Information to Identity Theft Victims* - Banks must provide records to victims pertaining to applications or transactions that were the result of an alleged identity theft. This helps an identify theft victim obtain the information necessary for investigation and law enforcement; and,
- *Prevention of Re-Pollution of Reports* - Banks must ensure that transaction history related to a fraudulent account is not re-reported to consumer reporting agencies once an investigation is underway.

Moreover, the agencies are continuing to work on additional regulations to implement other provisions of the FACTA that will aid in the prevention of, or response to, cases of identity theft.

The FDIC evaluates the banks' adherence to the FCRA as part of our compliance examinations. Like the GLBA Privacy rules, interagency procedures were developed through the FFIEC for evaluating compliance with the FCRA requirements. Part of the examination process includes verifying whether banks are obtaining consumer reports only for permissible purposes. Effective management of FCRA and other programs help to ensure that financial institution employees do not obtain reports on consumers without a legitimate business reason. Also, the examinations include evaluations of banks' information sharing activities with regard to consumer report information, to determine how this information is shared and with whom, and in turn, the related consumer disclosure requirements. Under the new FACTA requirements, we have begun evaluating banks' procedures to ensure that fraud and active duty alerts are properly handled when they appear on consumer reports received by the banks. Also, the banks' procedures for providing information on fraudulent accounts and transactions to victims of identity theft are also being evaluated during compliance examinations.

In March 2001, the federal banking agencies issued *Interagency Guidelines Establishing Information Security Standards*, as required by Section 501(b) of GLBA, requiring every financial institution to have a written information security program, approved by the institution's board of directors, to protect customer information. In addition, institutions must regularly test and update their security program. The institutions must conduct a risk assessment to identify foreseeable threats and vulnerabilities that could result in the unauthorized disclosure or misuse of sensitive customer information as well as an assessment of the likelihood and potential damage that could occur to that information. There is a requirement for a system of administrative, technical and physical controls designed to mitigate the risks identified, based on

the size and complexity of the institution and with regard to how data is collected, stored, used, transmitted, protected and disposed of. An assessment of arrangements with service providers that may have access to bank customer information also must be conducted. Further, the institutions are required to have an information security training program for employees. Finally, the institution must provide its board of directors with annual reports on the state of the security program.

FDIC IT examinations are conducted in accordance with guidance established by the FFIEC for national examination programs, or through guidance developed by the FDIC for financial institution examinations. The FFIEC, in partnership with the FDIC, has published a series of Information Technology Examination Handbooks. The handbooks address objectives, standards, resources, roles and responsibilities, best practices, and examination procedures. These handbooks are available to examiners, bankers, and the public and are an excellent resource to anyone trying to establish a data security program.

Information Technology examinations address a wide range of data security issues such as:

- Information security programs and compliance with GLBA requirements;
- IT audit coverage and independent review of controls;
- Practices for development and acquisition of software and IT services;
- Administrative controls and practices, such as IT security strategies and policies and personnel controls; and,
- Operational issues such as business continuity planning and physical security.

In addition, the FDIC has issued a variety of guidance to financial institutions with respect to keeping data secure, protecting customers, and responding to breaches of data security. For example, the federal banking agencies recently issued guidelines to implement Section 216 of FACTA. The guidelines are designed to protect consumers against risks associated with identity theft by requiring financial institutions to properly dispose of consumer information. Each financial institution is required to develop and maintain, as part of its information security program, appropriate controls to ensure that it properly disposes of consumer information derived from consumer reports. These guidelines are now included as an integral part of the *Interagency Guidelines Establishing Information Security Standards*. Each bank must satisfy these guidelines by July 1, 2005, and must modify any affected contract with service providers no later than July 1, 2006.

Guidance When Data Protection Fails

The federal banking agencies issued guidance in March 2005 for financial institutions to develop and implement a *Response Program* designed to address incidents of unauthorized access to sensitive customer information. This guidance is an interpretation of Section 501(b) of GLBA and its implementing guidelines. The Guidance states that at a minimum, the response program should contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;

- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Filing a timely Suspicious Activity Report (SAR) in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, and promptly notifying appropriate law enforcement authorities;
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and,
- Notifying customers in a clear manner, if the financial institution becomes aware of an incident of unauthorized access to the customer's information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or is reasonably possible to occur.

Under this Guidance, customer notice should be given in a clear and conspicuous manner and should include a description of the incident; the types of information subject to unauthorized access; measures taken by the financial institution to protect the customers from further unauthorized access; a telephone number customers can call for information and assistance; and, a reminder to customers to remain vigilant over the next 12 to 24 months, reporting any suspected identity theft incidents to the financial institution. The Guidance also encourages financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to large numbers of customers that include contact information for the reporting agencies.

Outreach

The FDIC has taken an active role in reaching large numbers of people in the financial sector to discuss cyber risks and controls. In the past three years, the FDIC has created several major outreach events:

- *Protecting the Financial Sector – A Public and Private Partnership* - The FDIC, along with other banking and financial sector regulators, are members of the FBIIC. The FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Member agencies communicate emerging issues and coordinate responses to emergency and other incidents. The FBIIC coordination effort is chaired by Department of Treasury and is chartered under the President's Working Group on Financial Markets. FBIIC coordinates with private sector organizations such as the Financial Sector Coordinating Council (FSCC) on significant information security events and incidents. The FDIC also works with Federal law enforcement agencies and regulators in both our outreach efforts and in response to specific incidents. In partnership with the FBIIC, the FDIC hosted a series of symposia examining the security of the U.S. financial sector and steps banks should take to protect themselves, including issues on cyber security. To date, the FDIC has hosted over 20 of these events around the country with over 1,000 bank executives attending.

- *FDIC Cyber Risk Management Symposium Series* - The FDIC created and hosted several outreach events to bring together government and industry to discuss current technology issues from a business perspective and a path for potential solutions. Topics have included offshore outsourcing of technology, electronic scams, incident response, information sharing, and other topics related to securing bank data.

- *Identity Theft Symposia* - The findings and recommendations of the FDIC Identity Theft study facilitated our efforts to lead the public policy and consumer education debate on identity theft. On February 11, 2005 the FDIC sponsored an identity theft symposium to coincide with the observance of National Consumer Protection Week. That symposium, attended by a standing room only group of industry representatives, consumer groups, state and local officials, academics and fellow regulators, prompted us to plan additional sessions. On May 13, 2005, the FDIC held the first of three regional symposia on this topic in Atlanta. Other symposia will follow in Los Angeles in June and Chicago in September, 2005. The symposia have brought together government, industry, law enforcement, and consumer interests to identify the scope of the identity theft problem and discuss proposed solutions. At the February 2005 symposium, the FDIC invited audience members and speakers to volunteer to participate in a consumer education focus group that will give us input on current consumer education efforts as well as consumer education needs in the area of identity theft.

- *Publications* - The FDIC frequently publishes articles on identity theft in its quarterly FDIC Consumer News. Various articles have covered cyber security from a consumer's

point of view, including how consumers can protect themselves against threats such as phishing, spyware and keystroke loggers. In addition to being available on our website, FDIC Consumer News has a circulation of over 60,000 (free of charge) and the information given is often cited by major publications, and news organizations.

Conclusion

In sum, the FDIC believes that we have the authority needed to address the risks of data security in the financial industry. No amount of legislation or regulation can completely eliminate the threat. However, we believe that our collaborative efforts with industry, the public, and our fellow regulators, will significantly minimize threats to data security. We stand ready to work with the Committee to provide assistance in any way to effectively address the elusive issues associated with data security.