Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-132-2004
December 14, 2004

IDENTITY THEFT

Study on "Account-Hijacking" Identity Theft and Suggestions for Reducing Online Fraud

Summary: The FDIC has issued a study on "account-hijacking" identity theft, which outlines the problem and suggests steps to reduce online fraud for both bank and regulatory agency consideration. The FDIC hopes to use the study to formulate guidance to bankers next year. Comments on the study are due on February 11, 2005.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Technology Officer
Chief Information Officer

Related Topics:
FFIEC Examination Handbook, E-Banking Booklet
FFIEC Examination Handbook, Information Security Booklet
Internet Banking Fraud, issued in FIL-113-2004 on September 13, 2004

Attachment:
None

Contact:
Jeffrey M. Kopchik, Senior Policy Analyst, at jkopchik@fdic.gov or 202-898-3872.

Send comments through February 11, 2005, via email to: IDTheftStudy@fdic.gov.

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2004/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-416-6940).

Highlights:

- The FDIC's study *Putting an End to Account-Hijacking Identity Theft* is now available.
- Account hijacking is the unauthorized access to and misuse of existing asset accounts and it occurs primarily through phishing and hacking. At this time, account hijacking is the fastest growing form of identity theft.
- Fraudsters are taking advantage of (1) bank reliance on single-factor authentication (i.e., using only one type of credential, such as a single password) for remote access to online banking, and (2) the lack of e-mail and Web site authentication to perpetrate account hijacking identity theft.
- Four suggested steps for reducing online fraud are offered, including:
  - Upgrading existing password-based single-factor customer authentication to two-factor customer authentication;
  - Using scanning software to identify and defend against phishing attacks;
  - Strengthening consumer educational programs; and
  - Continuing to emphasize information-sharing among the financial services industry, government agencies and technology providers.
- The FDIC study can be found on the Web at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html; comments on the study are due by February 11, 2005, via e-mail to IDTheftStudy@fdic.gov.

IDENTITY THEFT
Study on "Account-Hijacking" Identity Theft and Suggestions for Reducing Online Fraud

The Federal Deposit Insurance Corporation (FDIC) has produced the study *Putting an End to Account-Hijacking Identity Theft*, which outlines this form of identity theft and offers steps to reduce online fraud for both bank and regulatory agency consideration. The FDIC hopes to use the study to formulate guidance to bankers next year. The FDIC is seeking comments on the study by February 11, 2005.

Background and Focus of Study

Identity theft is one of the fastest growing types of consumer fraud. The Federal Trade Commission (FTC) has estimated that, during 2003, almost ten million Americans discovered that they were the victims of identity theft, with a total cost to businesses and consumers approaching $50 billion. This study focuses on a subset of identity theft that is of particular concern to FDIC-insured financial institutions and to their customers: the unauthorized access to and misuse of existing asset accounts primarily through phishing (which is the use of fraudulent e-mails to trick consumers into divulging confidential information) and hacking (which is the unauthorized remote access to a computer), hereinafter referred to as "account hijacking."

Prevalence and Impact of Account Hijacking

While precise statistics on the prevalence of account hijacking are difficult to obtain, recent studies indicate that unauthorized access to checking accounts is the fastest growing form of identity theft. The FTC has estimated that almost 2 million U.S. adult Internet users experienced this type of fraud during the 12 months ending in April 2004. Of those, 70 percent did their banking or paid their bills online and over half believed that they had received a phishing e-mail. Consumers are beginning to consider that their use of the Internet to conduct financial transactions may bring an increasing degree of risk, and many experts believe that electronic fraud, especially account hijacking, will slow the growth of online banking and commerce.

Findings

Fraudsters are taking advantage of the reliance on single-factor authentication for remote access to online banking, and the lack of e-mail and Web site authentication, to perpetrate account hijacking. Financial institutions and government agencies should consider a number of steps to reduce online fraud, including:

- Upgrading existing password-based single-factor customer authentication systems to two-factor authentication systems.

- Using scanning software to proactively identify and defend against phishing attacks. The further development and use of fraud detection software to identify account hijacking, similar to existing software that detects credit card fraud, could also help to reduce account hijacking.

- Strengthening educational programs to help consumers avoid online scams, such as phishing, that can lead to account hijacking and other forms of identity theft and taking appropriate action to limit their liability.

- Placing a continuing emphasis on information-sharing among the financial services industry, government agencies and technology providers.

The FDIC study can be found on the Web at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html; comments may be submitted via e-mail to IDTheftStudy@fdic.gov.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection