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

Financial Institution Letter
FIL-59-2005
July 5, 2005

IDENTITY THEFT
Study Supplement on "Account-Hijacking" Identity Theft

Summary: The FDIC has issued a supplement to its December 14, 2004, study on account-hijacking identity theft (see FIL-132-2004).

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.

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/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 supplement on account-hijacking identity theft is now available.
- The supplement reviews and responds to public comments on the original study.
- The supplement surveys the most recent trends in identity theft in general and account hijacking in particular.
- The supplement discusses authentication technologies that were not discussed in the study.
- The supplement presents two updated findings:
  - Information security risk assessment should include an analysis to determine whether the institution needs to implement more secure customer authentication methods and, if so, which methods are the most appropriate; and
  - If an institution offers retail customers 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 with a reliable form of multifactor authentication or other layered security.
- The FDIC study supplement can be found on the Web at: www.fdic.gov/consumers/consumer/idtheftstudysupp/index.html.

IDENTITY THEFT
Study Supplement on "Account-Hijacking" Identity Theft

The Federal Deposit Insurance Corporation (FDIC) has published a supplement to its December 14, 2004, study *Putting an End to Account-Hijacking Identity Theft* (see FIL-132-2004).

Background and Focus of Supplement

The supplement was published to review and respond to public comments received about the original study, to survey the most recent trends in identity theft, to discuss authentication technologies that were not discussed in the original study, and to present two updated findings.

Prevalence and Impact of Account Hijacking

The supplement concludes that identity theft and account hijacking continue to be significant problems for the financial services industry and consumers. Consumers are having more difficulty protecting themselves from identity theft as it continues to evolve in complex ways. Consumers are concerned about online security and may be receptive to using two-factor authentication if they perceive that this method offers improved safety and convenience.

Findings

Each financial institution may choose a different solution to address account-hijacking identity theft, or each may choose a variety of solutions based on the institution's complexity and the nature and scope of its activities. The FDIC does not intend to propose one solution for all. However, the evidence examined in the supplement 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:

- 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. which method or methods make the most sense in view of the nature of the institution's business and customer base.

- 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 a user ID and a 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.

The FDIC supplement can be found on the Web at:
www.fdic.gov/consumers/consumer/idtheftstudysupp/index.html.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection