PRESS RELEASE

Federal Deposit Insurance Corporation

FOR IMMEDIATE RELEASE
June 27, 2005

Media Contact:
David Barr (202) 898-6992

Latest FDIC Findings on Identity Theft Suggest Need for New Safeguards for Internet Banking

"User names" and passwords should be supported in Internet banking transactions with new and better ways of identifying real customers from fraud artists trying to "highjack" bank accounts, according to an update on identity theft from the Federal Deposit Insurance Corporation (FDIC).s

"Identity theft, particularly account hijacking, continues to grow as a problem for the financial services industry and for consumers," said FDIC Chairman Don Powell. "Our review illustrates that ID theft is evolving in more complicated ways and that more can and should be done to make online banking more secure."

The new findings are in a supplement to an FDIC study issued in December about ways to fight "phishing" scams, in which criminals send fraudulent e-mails to trick consumers into providing confidential financial information that can lead to illegal access to bank accounts. The supplement reviews and responds to public comments that the FDIC received about the original study, identifies the most recent trends in identity theft, and discusses a variety of new technologies that could be used to make Internet banking more secure.

In the latest findings, the FDIC concluded that the risk assessment financial institutions are required to perform regarding information security also should address customer authentication. The supplement also said that if an institution offers Internet banking, it has an obligation to properly secure that delivery channel. This extra level of security for online accounts, often referred to as "multifactor authentication," would be used in addition to the traditional passwords. These new security features may include "tokens" issued to customers that generate new passwords every 60 seconds, software that can identify the computer that a customer uses to access online accounts, or contacting a customer by phone to make sure that he or she is the one attempting to access the account.

FDIC

Congress created the Federal Deposit Insurance Corporation in 1933 to restore public confidence in the nation's banking system. It promotes the safety and soundness of these institutions by identifying, monitoring and addressing risks to which they are exposed. The FDIC receives no federal tax dollars — insured financial institutions fund its operations.

FDIC press releases and other information are available on the Internet at www.fdic.gov, by subscription electronically (go to www.fdic.gov/about/subscriptions/index.html) and may also be obtained through the FDIC's Public Information Center (877-275-3342 or 703-562-2200). PR-58-2005

The FDIC and other federal banking agencies are expected to issue guidance this fall to insured financial institutions about improving the security of customer authentication methods. The latest FDIC findings are expected to be considered in the development of that guidance.

"The FDIC does not intend to propose one solution for all, but the evidence…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 supplement said. It added that consumers are concerned about online security and may be receptive to using a new form of authentication "if they perceive it as offering improved safety and convenience."

The supplement is available on the Web at:
www.fdic.gov/consumers/consumer/idtheftstudysupp/index.html.