Board Of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Joint Release **Office of Thrift Supervision**

NR 2004-77
For Immediate Release
September 8, 2004

Federal Bank, Thrift and Credit Union Regulatory Agencies Provide Brochure with Information on Internet "Phishing"

The federal bank, thrift and credit union agencies today announced the publication of a brochure with information to help consumers identify and combat a new type of Internet scam known as "phishing."

The term is a play on the word "fishing," and that's exactly what Internet thieves are doing – fishing for confidential financial information, such as account numbers and passwords. With enough information, a con artist can run up bills on another person's credit card or, in the worst case, even steal that person's identity.

In a common type of phishing scam, individuals receive e-mails that appear to come from their financial institution. The e-mail may look authentic, right down to the use of the institution's logo and marketing slogans. The e-mails often describe a situation that requires immediate attention and then warn that the account will be terminated unless the e-mail recipients verify their account information immediately by clicking on a provided link.

The link will take the e-mail recipient to a screen that asks for account information. While it may appear to be a page sponsored by a legitimate financial institution, the information will actually go to the con artist who sent the e-mail.

The federal financial regulatory agencies want consumers to know that they should never respond to such requests. No legitimate financial institution will ever ask its customers to verify their account information online.

The brochure also advises consumers:

- Never click on the link provided in an e-mail if there is reason to believe it is fraudulent. The link may contain a virus.
- Do not be intimidated by e-mails that warn of dire consequences for not following their instructions.
- If there is a question about whether the e-mail is legitimate, go to the company's site by typing in a site address that you know to be legitimate.
- If you fall victim to a phishing scam, act immediately to protect yourself by

alerting your financial institution, placing fraud alerts on your credit files and monitoring your account statements closely.

- Report suspicious e-mails or calls to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

The interagency brochure is available on each agency's web site and financial institutions are encouraged to download the camera-ready file for use in their own customer-education programs.

# # #

Attachment

Media Contacts:

Federal Reserve	Susan Stawick	(202) 452-2955
FDIC	David Barr	(202) 898-6992
NCUA	Cherie Umbel	(703) 518-6330
OCC	Kevin Mukri	(202) 874-5770
OTS	Erin Hickman	(202) 906-6677