

FEDERAL RESERVE BANK OF SAN FRANCISCO
101 MARKET STREET, SAN FRANCISCO, CALIFORNIA

September 22, 2004

**BANKING SUPERVISION AND REGULATION:
INTERNET PHISHING SCAMS**

To State Member Banks, Bank
Holding Companies, U.S. Branches
and Agencies of Foreign Banks,
and Others Concerned,
in the Twelfth Federal Reserve District

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

The federal bank, thrift and credit union agencies have published 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,” which is 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 emails that appear to come from their financial institution. The email may look authentic, even using the institution’s logo and marketing slogans. The emails often describe a situation that requires immediate attention and then warn that the account will be terminated unless the email recipients verify their account information immediately by clicking on a provided link.

The link will take the email 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 email.

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 the following information:

- Never click on the link provided in an email if there is reason to believe it is fraudulent. The link may contain a virus.
- Do not be intimidated by emails that warn of dire consequences for not following their instructions.
- If there is a question about whether the email 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 emails 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, such as <http://www.occ.gov/consumer/phishing.htm>, and financial institutions are encouraged to download the camera-ready file for use in their own customer-education programs.

Additional Information

All circulars and documents are available on the Internet through the Federal Reserve Bank of San Francisco's Internet site, at <http://www.frbsf.org/banking/letters>.

For additional information about phishing, please contact our Banking Supervision and Regulation Department at (415) 974-3028.

FEDERAL RESERVE BANK OF SAN FRANCISCO