BOARD OF GOVERNORS

OF THE

FEDERAL RESERVE SYSTEM

WASHINGTON, D.C. 20551

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 04 - 14

CA 04- 7

October 19, 2004

TO THE OFFICER IN CHARGE OF SUPERVISION AT EACH FEDERAL RESERVE BANK AND TO EACH DOMESTIC AND FOREIGN BANKING ORGANIZATION SUPERVISED BY THE FEDERAL RESERVE

SUBJECT: FFIEC Brochure with Information on Internet "Phishing"

The federal banking, thrift, and credit union regulatory agencies have published an informational brochure to assist consumers in identifying and preventing a new type of Internet fraud known as "phishing."

Phishing involves the fraudulent acquisition and use of an individual's personal or financial information. In a common type of phishing scam, individuals receive e-mail messages that appear to have been initiated by their financial institution. These messages may look authentic and often include the institution's logo and marketing slogans. The e-mail messages usually describe a situation that requires immediate attention and state that the accounts will be terminated unless the recipients verify their account information immediately by clicking on a provided web link.

The web link then takes the e-mail recipients to a screen that asks for personal or financial information including account numbers, Social Security numbers, passwords, place of birth, or other information used to identify the consumers. Those perpetrating the fraud then use this information to access consumers' accounts or assume the consumers' identities.

The brochure explains the basics of "phishing," the steps consumers can take to protect themselves, and the actions that consumers can take if they become a victim of identity theft. The brochure, *Internet Pirates Are Trying to Steal Your Information*, is available in a downloadable form through the Federal Reserve Board's Web site at http://www.federalreserve.gov/consumers.htm.

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 from third parties to the Federal Trade Commission either through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

Reserve Banks are asked to distribute this guidance to banking organizations supervised by the Federal Reserve. If you have any questions regarding this letter, please contact Suzanne Killian, Manager, Oversight Section, Division of Consumer and Community Affairs, (202) 452-2090, Adrienne Haden, Manager, Operational and Information Technology Risk, Division of Banking Supervision and Regulation, (202) 452-2058, or Donna Parker, Supervisory Financial Analyst, Division of Banking Supervision and Regulation, (202) 452-2614.

Richard Spillenkothen
Director
Division of Banking Supervision
and Regulation

Sandra Braunstein
Director
Division of Consumer and
Community Affairs