

**Office of Thrift Supervision**Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*

1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

September 8, 2004

MEMORANDUM FOR: CHIEF EXECUTIVE OFFICERS**FROM:**

Scott M. Albinson

SUBJECT:

Phishing Customer Brochure

PURPOSE

As thrift customers increasingly use the Internet to perform banking functions, criminals are using more sophisticated methods to steal customers' passwords, access codes and to obtain other personal and confidential information (e.g., names, addresses, Social Security numbers). To assist you in raising customer awareness, the Office of Thrift Supervision (OTS) and other Federal Financial Institutions Examination Council (FFIEC) member agencies have developed the brochure outlining steps thrift and other depository institution customers can take to reduce the risk of identity theft.

BACKGROUND

The Anti-Phishing Working Group (an industry organization, <http://www.antiphishing.org>), reports that identity theft frauds known as "phishing" attacks have increased significantly over the last year. Phishing is a term used for criminals' attempts at stealing personal financial information through fraudulent e-mails and Websites designed to appear as though they were generated from legitimate businesses, financial institutions, and government agencies.¹ These scams are contributing to a rise in identity theft, credit card fraud, and other Internet-based frauds. E-commerce customers, including customers of financial institutions, have fallen victim to these scams.

Thrifts are encouraged to implement programs to educate their customers about phishing attacks and related types of online fraud to help customers avoid becoming victims of these illegal activities. These educational programs should include information to help customers identify the potential risks associated with identity theft, as well as provide examples of the most frequently used fraudulent schemes. In addition, thrifts should encourage their customers to inform the institution when customers encounter fraud or potentially fraudulent schemes.

¹ CEO Memo 193, Phishing and E-Mail Scams, March 8, 2004

The brochure is available to supplement thrifts' customer education efforts. The brochure, which can be used as a deposit and loan statement stuffer, identifies the risks of identity theft and the steps customers should take to reduce their chances of becoming victims. The brochure also outlines practical steps customers should take if they fall victim to phishing attacks.

OTS encourages thrifts to consider using this brochure by distributing it to customers and/or posting it to their Website. Thrifts are encouraged to provide customers additional relevant educational information deemed appropriate. A "camera-ready" version of the attached brochure is available on the OTS Web site at <http://www.ots.treas.gov/docs/4/48951.pdf>.

For questions concerning Internet fraud and phishing attacks, please contact Robert Engebret, Director Information Technology Risk and Critical Infrastructure Protection at (202) 906-5631.