



SA-205-2008

October 28, 2008

SPECIAL ALERT

TO: CHIEF EXECUTIVE OFFICER

SUBJECT: Phishing Scams Involving Financial Institutions in the News

Summary: *Fraudulent phishing e-mails claiming to be from, or related to, financial institutions involved in high-profile mergers, acquisitions or failures are reportedly in circulation.*

The Federal Deposit Insurance Corporation (FDIC) is warning consumers, businesses and financial institutions to be aware of fraudulent e-mails allegedly from, or related to, financial institutions that have been the subject of recent news stories. Phishing e-mails often incorporate aspects of high-profile news stories – such as bank mergers, acquisitions and failures – to create a sense of urgency and legitimacy for requesting information or action.

These types of fraudulent e-mails may request recipients to verify computer logon credentials, update personal information, or activate new online security features. The fraudulent e-mails may include a link that directs the recipient to a fraudulent or “spoofed” Web site that looks similar to the subject institution’s legitimate Web site. Once there, users may be prompted to provide information about online banking credentials or other personal and confidential information that could be used to gain unauthorized access to online banking services or perpetrate identity theft. These spoofed Web sites may also direct the user to download software updates or digital certificates, which may actually be malicious code or software attempting to collect online banking credentials or other personal and confidential information.

Consumers, businesses and financial institutions should be wary of unsolicited e-mails purportedly from financial institutions recently in the news and take the following precautions:

- Do not follow Web links in unsolicited e-mails from apparent financial institutions. Instead, use Web browser bookmarks or type your institution’s Web address into the browser address bar when accessing your bank’s Web site or online banking services.
- Always use anti-virus software and ensure the virus signatures are automatically updated. Ensure the computer operating system and common software applications are up-to-date with security patches installed.
- Do not open unsolicited or unexpected e-mail attachments claiming to be from a financial institution because of the risk of malicious code or software. As a precaution, call the financial institution using an appropriate telephone number, such as one from an account statement, to validate the e-mail and attached file before opening any attachment.

- Be aware that phishing e-mails frequently use new and innovative ways to trick recipients into providing logon credentials and confidential information or into unleashing malicious code.
- Regularly review financial account statements and immediately report any discrepancies to your institution.
- Be mindful that financial institutions generally deliver notices to consumers in writing about changes in account terms and conditions unless the consumer previously agreed to receive the notice electronically.

For additional information about safe online banking and avoiding online scams, visit <http://www.fdic.gov/consumers/consumer/guard/>.

For your reference, FDIC Special Alerts may be accessed from the FDIC's Web site at www.fdic.gov/news/news/SpecialAlert/2008/index.html. To learn how to automatically receive FDIC Special Alerts via e-mail, please visit www.fdic.gov/about/subscriptions/index.html.

Sandra L. Thompson
Director
Division of Supervision and Consumer Protection

Distribution: FDIC-supervised Banks (Commercial and Savings)

Paper copies of FDIC Special Alerts may be obtained through the FDIC's Public Information Center, 1-877-275-3342 or 703-562-2200.