



SA-266-2006

September 14, 2006

SPECIAL ALERT

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)

SUBJECT: Fraudulent E-Mail Claims to Be From the FDIC

Summary: *E-mails that fraudulently claim to be from the FDIC are requesting that recipients provide highly sensitive personal information, including bank account information.*

The Federal Deposit Insurance Corporation (FDIC) has become aware of e-mails appearing to be from the FDIC asking recipients to register for a “SON – Secure Online Network” code. The e-mail requests that recipients click on a hyperlink to initiate “SON” registration in an attempt to acquire the recipients’ personal financial information. These e-mails are fraudulent and were not sent by the FDIC. Financial institutions and consumers should NOT access the link provided within the body of these e-mails and should NOT, under any circumstances, provide any personal financial information through this media.

The fraudulent e-mails describe a fictitious relationship between the FDIC and GoldLeaf Financial Solutions and suggest that the FDIC collaborated in the development of SON. The e-mails state that “SON”:

- is “dedicated to protect payment cards against online fraud”;
- “assigns a unique code to a payment card, therefore replacing random parts of the personal information”; and
- is “required for FDIC claims as it is part of the FDIC’s new set of standards.”

Variations of the e-mails have been reported. For example, at least three different subject lines are currently being used, including “Urgent Notification - Security Reminder,” “Online Access Agreement Update,” and “SON Registration.” Some versions of the fraudulent e-mails include a salutation of “Dear FDIC beneficiary,” while other versions include the recipient’s name and e-mail address after the word “Dear.” Some versions of the e-mails include the recipient’s name and mailing address and a statement that “your personal information did not match any SON code.” Other subject lines and modifications to the e-mails may occur over time.

Financial institutions and consumers should be aware that other similar e-mails may be sent that falsely claim to be from the FDIC. The FDIC does not directly contact consumers in this manner nor does the FDIC request personal financial information from consumers.

The FDIC is attempting to identify the source of the fraudulent e-mails and disrupt the transmission. Until this is achieved, consumers and financial institutions should notify the FDIC at alert@fdic.gov of any similar attempts to obtain personal financial information.

Information about counterfeit items, cyber-fraud incidents and other fraudulent activity may be forwarded to the FDIC's Cyber-Fraud and Financial Crimes Section, 550 17th Street, N.W., Room F-4004, Washington, D.C. 20429, or transmitted electronically to alert@fdic.gov. Information related to federal deposit insurance or consumer issues should be submitted to the FDIC using an online form that can be accessed at <http://www2.fdic.gov/starsmail/index.asp>.

For your reference, FDIC Special Alerts may be accessed from the FDIC's website at www.fdic.gov/news/news/SpecialAlert/2006/index.html. To learn how to automatically receive FDIC Special Alerts through e-mail, please visit www.fdic.gov/about/subscriptions/index.html.

Sandra L. Thompson
Acting Director
Division of Supervision and Consumer Protection

Distribution: All FDIC-Insured Institutions

NOTE: Paper copies of FDIC Special Alerts may be obtained through the FDIC's Public Information (1-877-275-3342).