FRAUD ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: **January 2009** **Fraud ALERT NO.: 09-Fraud-01**

TO: **Federally-Insured Credit Unions**

SUBJ: **Fedwire Phishing Scheme**

REF: **Federal Deposit Insurance Corporation, Special Alert SA-20-2009, Fedwire Phishing Scheme**

Dear Board of Directors:

The National Credit Union Administration is warning credit unions to be aware of fraudulent e-mails allegedly from the Federal Reserve Bank. The fraudulent e-mails claim that a phishing attack has affected the Fedwire system and that restrictions are in place. The e-mails further instruct recipients to click on links within the e-mail for additional information.

The fraudulent e-mails have included various spoofed names and addresses in the "From:" line of the messages, including "Bank System Administration," "System Administration", and "Federal Reserve Bank." The e-mails contain the following message verbatim:

> FEDERAL RESERVE BANK
>
> Important:
>
> You're getting this letter in connection with new directives issued by U.S. Treasury Department. The directives concern U.S. Federal Wire online payments.
>
> On On January 1, 2009 a large-scaled phishing attack started and has been still lasting. A great number of banks and credit unions is affected by this attack and quantity of illegal wire transfers has reached an extremely high level.
>
> U.S. Treasury Department, Federal Reserve and Federal Deposit Insurance Corporation (FDIC) in common worked out a complex of immediate actions for the highest possible reduction of fraudulent operations. We regret to inform you

that definite restrictions will be applied to all Federal Wire transfers from January 6 till January 16.

Here you can get more detailed information regarding the affected banks and U.S. Treasury Department restrictions:

The message contains links to two Web pages that attempt to load malicious Trojan horse programs onto end users' computers.

Credit unions should be aware that Fedwire operations are not restricted and are operating as normal, and should take the following precautions:

- If an end user received the e-mail and clicked on any of the links, fully scan the computer using updated anti-virus software. If malicious code is detected on the computer, consult with a computer security or anti-virus specialist to remove the malicious code or re-install a clean image of the computer system.
- Be aware that phishing e-mails frequently have links to Web pages that host malicious code and software. Do not follow Web links in unsolicited e-mails from apparent federal banking agencies. Instead, bookmark or type the agency's Web address.
- Always use anti-virus software and ensure that the virus signatures are automatically updated. Ensure that the computer operating systems and common software applications security patches are installed.
- Do not open unsolicited or unexpected e-mail attachments because of the risk of malicious code or software in the attachments. Instead, call the agency using a known and appropriate telephone number to verify the legitimacy of the message and attached file.
- Be alert to different variations of the fraudulent e-mails.

Additional information regarding fraudulent schemes and reporting such activity can be found on NCUA's website at http://www.ncua.gov/FraudInfo/index.htm. Using that link, you will find other NCUA issued Fraud Alerts as well as an option for federally-insured credit unions to subscribe to receive NCUA publications automatically through e-mail.

Sincerely,

/ S /

John E. Kutchey
Acting Director of Examination & Insurance