NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: **April 2004** **LETTER NO.: 04-CU-05**

TO: **Federally Insured Credit Unions**

SUBJ: **Fraudulent E-Mail Schemes**

Dear Board of Directors:

This letter is to inform you that the United States Department of Treasury has issued a press release regarding recent fraudulent e-mail schemes designed to deceive consumers into surrendering sensitive personal information which could lead to identity theft.

Fraudulent e-mails, which may appear to be from government agencies, direct recipients, such as credit union members, to websites where they are asked to verify personal information such as name, account and credit card numbers, passwords, social security numbers and other information. These websites often appear to be very similar to official government sites; however, they are not authentic official sites and are intended only to steal the member's information.

These e-mails are part of a scam known as "phishing." Phishing is a high-tech scam where e-mails are sent to consumers falsely claiming to be a legitimate company, in an attempt to obtain non-public personal information. The e-mails may claim the information is needed to assist in the fight against terrorism or some other purpose supposedly required by law. However, NCUA wants to assure credit union members that federal financial agencies do not use e-mail as a means of communicating requests for sensitive personal information.

In an ongoing effort to combat identity theft, several tips developed by the Federal Trade Commission (FTC) are listed below which may help your members protect themselves from becoming a victim of this latest scam.

- If a member receives an e-mail that warns them, with little or no notice, that an account of theirs will be shut down unless they reconfirm their billing information, they should not reply or click on the link in the e-mail. Instead, they should contact the company cited in the e-mail directly using a telephone number or website address they know to be genuine.

- Members should avoid e-mailing personal and financial information. Before submitting financial information through a website, they should look for the "lock" icon on the browser's status bar. NCUA also suggests looking for "https" in the website address. Both of these indicators signal the information is secure during transmission.
- Members should review credit card and credit union account statements as soon as they receive them to determine whether there are any unauthorized charges. If the statement is late by more than a couple of days, members should call the credit card company or credit union to confirm their billing address and account balances.
- Members should report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov. If they believe they have been a victim of a fraudulent scheme, they should file a complaint at www.ftc.gov, and the visit the FTC's Identity Theft website (www.ftc.gov/idtheft) to learn how to minimize their risk of damage from the identity theft.

NCUA encourages you to inform your members of these schemes and how they can protect themselves. Also, please assure them that neither NCUA nor any other federal financial agency uses e-mail to request non-public information such as account numbers, date of birth, or social security number.

The press release on this subject can be found on the United States Department of Treasury's website at www.ustreas.gov/press/releases/js1130.htm.

Should you have any questions regarding this subject, please do not hesitate to contact your Regional Director or State Supervisory Authority.

Sincerely,

/S/

Dennis Dollar
Chairman