NCUA LETTER TO CREDIT UNIONS

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

DATE: September 2004 **LETTER NO.: 04-CU-12**

TO: Federally Insured Credit Unions

SUBJ: Phishing Guidance for Credit Union Members

ENCL: FFIEC Phishing Brochure

DEAR BOARD OF DIRECTORS:

As credit union members increasingly use the Internet to perform financial services functions, criminals are using more sophisticated methods to steal members' passwords, access codes and to obtain other personal and confidential information (e.g., names, addresses, Social Security numbers). In our most recent Letter to Credit Unions #04-CU-06 E-Mail and Internet Related Fraudulent Schemes Guidance, we highlighted the need to educate your membership about such activities. To assist credit unions' efforts in raising member awareness, the NCUA and other Federal Financial Examination Council (FFIEC) member agencies[1] have developed the enclosed brochure outlining steps credit union members should take to reduce the risk of identity theft.

An industry organization, the Anti-Phishing Working Group (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. These scams are contributing to a rise in identity theft, and credit card and other Internet-based frauds. E-commerce customers, including credit union members, have fallen victim to these scams.

[1] Federal Financial Institution Examination Council member agencies include Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

Credit unions should have information readily available to educate their members about phishing attacks and related types of online fraud to help members avoid becoming victims of these illegal activities. These educational programs should include information to help members identify the potential risks associated with identity theft, as well as descriptions of the most frequently used fraudulent schemes. Informed members can help credit unions identify many types of fraud.

The attached brochure can be used to supplement your member education efforts. The brochure, which can be used as a share and loan statement stuffer, identifies identity theft risks and the steps members should take to reduce their chances of becoming victims. The brochure also outlines practical steps members should take if they fall victim to phishing attacks.

The NCUA encourages credit unions to consider using this brochure, by either distributing the actual brochure to members or posting it to their Website. Credit unions should also provide members additional relevant educational information deemed appropriate. A "camera-ready" version of the brochure is available on the NCUA Web site at http://www.ncua.gov/Publications/brochures/IdentityTheft for downloading and copying. For credit unions that do not have access to the Internet, limited copies of the brochure can be obtained directly by contacting:

National Credit Union Administration
Office of the Chief Financial Officer – Division of Procurement and Facilities Management
1775 Duke Street
Alexandria, VA
Telephone: (703) 518-6340

Should you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/

JoAnn M. Johnson
Chairman

Enclosure