NCUA LETTER TO CREDIT UNIONS

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

DATE: April 2004 **LETTER NO.: 04-CU-06**

TO: Federally Insured Credit Unions

SUBJ: E-Mail and Internet Related Fraudulent Schemes Guidance

REF: Letter to Credit Unions #04-CU-05 Fraudulent E-Mail Schemes

Dear Board of Directors:

The purpose of this Letter is to provide additional guidance for combating the email schemes discussed in the recently released Letter to Credit Unions #04-CU-05 Fraudulent E-Mail Schemes. In addition, this Letter is intended to raise awareness of the increasingly common Internet fraud called "phishing." NCUA encourages credit unions to educate their members, strengthen monitoring systems, and enhance response programs to reduce the potential risk of Internet-related fraud schemes to their organization and members. Such schemes may negatively impact your credit union's reputation, transaction, liquidity, and strategic risks.

Background

The FBI's Internet Fraud Complaint Center (IFCC) reports a steady increase in complaints involving unsolicited e-mails directing consumers to a false "member service" website or directly asking for member information. These scams contribute to a rise in identity theft, credit card fraud, and other Internet-based frauds[1].

One type of Internet fraud, known as phishing, involves sending members a seemingly legitimate e-mail request for account information, often under the guise of asking the member to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information. In the e-mail, the perpetrator uses various means to convince members that they are receiving a legitimate message from someone whom the member may already be doing business with, such as a credit union. Techniques such as a false "From" address or the use of seemingly legitimate credit union logos, web links, and graphics may be employed to mislead the member.

[1] Federal Bureau of Investigation Press Release, "FBI Says web 'Spoofing' Scams are a Growing Problem", July 21, 2003.

After gaining the member's trust, the perpetrator attempts to convince the member to provide personal information and provides one or more methods for the member to communicate that information. For example, the e-mail might include a link to the perpetrator's website that contains a form for entering personal information. Like the e-mail, the website is designed to deceive the member into believing it is the credit union's website or a party affiliated with the credit union. Alternatively, the e-mail might simply include an embedded form for the member to complete. The ultimate goal of this fraud is to obtain and use the member information to gain unauthorized access to a member's credit union or financial accounts or to engage in other illegal acts.

Risks Associated With E-Mail and Internet-Related Fraudulent Schemes

Internet-related fraudulent schemes present a substantial reputation risk to a credit union that is falsely impersonated. Credit union members and potential members may mistakenly perceive that weak information security resulted in security breaches that allowed someone to obtain confidential information from the credit union. Potential negative publicity regarding an credit union's business practices may cause a decline in the credit union's member base, a loss in confidence, or result in costly litigation.

In addition, members who fall prey to e-mail and Internet-related fraudulent schemes face real and immediate risk. Criminals will normally act quickly to gain unauthorized access to financial accounts, commit identity theft, or engage in other illegal acts before the victim realizes the fraud has occurred and takes action to stop it.

Educating Credit Union Members About E-Mail and Internet-Related Fraudulent Schemes

Credit unions are encouraged to consider the merits of educating members about prevalent e-mail and Internet-related fraudulent schemes, such as phishing, and how to avoid them. This education effort may be accomplished in a number of ways that include the posting of notices on websites and the use of statement stuffers. Appropriate education and prevention efforts should convey the following messages:

- A credit union's web page should not be accessed from a link provided by a third party. It should only be accessed by typing the website name, or URL address, into the web browser or by using a "bookmark" that directs the web browser to the credit union's website.

- A credit union should not send e-mail messages requesting confidential information, such as account numbers, passwords, or personal identification numbers (PINs). Credit union members should be reminded to report any such requests to the credit union.

- Credit unions should maintain current website certificates[2] and describe how the member can authenticate the credit union's web pages by checking the properties on a secure web page.

To help explain the red flags and potential risks associated with phishing and identity theft, credit unions can refer members to, or use resources distributed by, the Federal Trade Commission (FTC), which include the following FTC brochures:

- "How Not to Get Hooked by the 'Phishing' Scam," published in July 2003, which is available at: http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

- "ID Theft: When Bad Things Happen to Your Good Name," published in September 2002, which is available at: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Responding to E-Mail and Internet-Related Fraudulent Schemes

Credit unions are encouraged to consider enhancing incident response programs to address possible e-mail and Internet-related fraudulent schemes. Enhancements may include:

- Incorporating notification procedures to alert members of known e-mail and Internet-related fraudulent schemes and to caution them against responding;

- Establishing a process to notify Internet service providers, domain name-issuing companies, and law enforcement to shut down fraudulent websites and other Internet resources that may be used to facilitate phishing or other e-mail and Internet-related fraudulent schemes;

- Increasing suspicious activity monitoring and employing additional identity verification controls;

- Offering members assistance when fraud is detected in connection with member accounts;

- Notifying the proper authorities when e-mail and Internet-related fraudulent schemes are detected, including promptly notifying their NCUA Regional Office and the appropriate law enforcement agencies; and

- Filing a Suspicious Activity Report when incidents of e-mail and Internet-related fraudulent schemes are suspected.

Steps Credit Unions Can Take to Mitigate Risks Associated With E-Mail and Internet-Related Fraudulent Schemes

[2] Website certificates, or "seals", are generally issued by third-party companies and are intended to assure online members that your website has been authenticated by the third party and that confidential transactions through your website are secured by SSL (secure sockets layer) encryption. Members may verify the validity of the certificate by clicking on the certificate logo.

To help mitigate the risks associated with e-mail and Internet-related fraudulent schemes, credit unions are advised to take steps to implement appropriate information security controls as described in the Financial Institutions Examination Council's (FFIEC) "Information Security Booklet" (available at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html). Specific actions that should be considered to prevent and deter e-mail and Internet-related fraudulent schemes include:

- Improving authentication methods and procedures to protect against the risk of user ID and password theft from members through e-mail and other frauds;

- Reviewing and, if necessary, enhancing practices for protecting confidential member data;

- Maintaining current website certificates and describing how members can authenticate the credit union's web pages by checking the properties on a secure web page;

- Monitoring accounts individually or in aggregate for unusual account activity such as address or phone number changes, a large or high volume of transfers, and unusual member service requests;

- Monitoring for fraudulent websites using variations of the credit union's name;

- Establishing a toll-free number for members to verify requests for confidential information or to report suspicious e-mail messages; and

- Training member service staff to refer member concerns regarding suspicious e-mail request activity to security staff.

Additional information concerning Internet-related fraud may be found in the following NCUA Letters to Credit Unions:

- 04-CU-05 Fraudulent E-Mail Schemes;

- 03-CU-12 Fraudulent Newspaper Advertisements, and websites by Entities Claiming to be Credit Unions;

- 02-CU-16 Protection of Credit Union Internet Addresses;

- 01-CU-09 Identity Theft and Pretext Calling; and

- 00-CU-02 Identity Theft Prevention.

Should you have any questions or concerns, please do not hesitate to contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/S/

Dennis Dollar
Chairman

FFIEC IT Examination Handbook

Gray titles indicate booklets that will be released at a future date.

Booklets

Audit	Management
Business Continuity Planning	Operations
Development and Acquisition	Outsourcing
E-Banking	**Retail Payment Systems**
FedLine	**Supervision of Technology Service Providers**
Information Security	Wholesale Payment Systems

Audit

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Business Continuity Planning Booklet

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations
- Non-regulatory Resources

Development and Acquisition

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

E-Banking

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- E-Banking Request Letter Items - Generic word-processing version
- E-Banking Request Letter Items - Microsoft Word 2000 version
- Presentations

FedLine

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Information Security Booklet

- Printable version of booklet
- Low resolution version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations
- Non-regulatory Resources

Management

Operations

Outsourcing

Retail Payment Systems

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations
- Non-regulatory Resources

Supervision of Technology Service Providers Booklet

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Wholesale Payment Systems