FRAUD ALERT

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

DATE: **January 2008** **Fraud ALERT NO.: 08-Fraud-01**

TO: **Federally-Insured Credit Unions**

SUBJ: **Identify Theft - Fraudulent Home Equity Line of Credit & Wire Transfer Activity**

Dear Board of Directors:

The purpose of this fraud alert is to inform all federally-insured credit unions about recent fraudulent activity involving members with Home Equity Line of Credit (HELOC) accounts. Several financial institutions, including credit unions, have reported fraudulent wire transfers performed on HELOC accounts. Typically, the imposter obtained publicly available HELOC information (from filings with state and local government entities), and combined with social engineering tactics, obtained access to member accounts, initiated a draw on the member's HELOC account, and subsequently initiated a wire transfer from the account.

In cases reported to NCUA, the imposter contacted the credit union and provided sufficient information to a credit union representative to gain access to a member's account. Once the imposter had access, he/she requested a transfer from the member's HELOC account to another transaction account (such as the member's checking account). These funds were then wire transferred out of the credit union.

Some of the scams have included a high level of sophistication which assisted the imposter in bypassing certain authentication controls. For example, the imposter has the ability to fool Caller ID software by making it appear that the call initiates from the account holder's valid phone number. Another example is the imposter was knowledgeable of recent account activity (such as deposit or withdrawal amounts) and used such information to authenticate himself/herself as the account holder to the credit union representative.

Credit union management should warn their member facing employees about this recent fraudulent activity. Management should ensure sufficient controls[1] are in place to ensure the proper authentication of members. Management should also ensure their staff are properly trained in recognizing questionable activity on member accounts. Management should be aware there may be variants to the scam previously described (i.e. not just involving HELOC accounts).

Where appropriate, management must ensure they file a Suspicious Activity Report in accordance with established regulation. As specified by NCUA Rules & Regulations Part 748, management must provide notice to the appropriate NCUA Regional Director, and in the case of state-chartered credit unions, to their state supervisory authority. Management should also contact and file a report with local law enforcement authorities.

NCUA will continue to follow this issue and provide you with additional information as warranted. In the meantime, if you have any questions, please contact your District Examiner, Regional Office, or State Supervisory Authority.

Sincerely,

David M. Marquis
Director of Examination & Insurance

[1] Controls could include a contact verification procedure wherein the credit union representative calls, or emails, the account holder to confirm the transaction prior to initiating the transaction. The representative should only use the member's contact information on file at the credit union.