NCUA LETTER TO CREDIT UNIONS

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

DATE: August 2006 **LETTER NO.: 06-CU-13**

TO: Federally Insured Credit Unions

SUBJ: Authentication for Internet Based Services

ENCL: Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment

REF: NCUA Letter To Credit Unions #05-CU-18 Guidance on Authentication in Internet Banking Environment

Dear Board of Directors:

NCUA issued Letter to Credit Unions 05-CU-18 Guidance on Authentication in Internet Banking in November 2005. The letter directs credit unions which provide Internet-based service to determine if appropriate authentication methodologies and technologies are in place to authenticate members. Credit unions should be in compliance with this letter by yearend 2006.

Credit unions providing Internet-based services to members should complete a risk assessment of those products and services to determine if high-risk transactions are performed. High-risk transactions are defined as access to member information or the movement of funds to other parties. The risk evaluation should consider at least the member transactional capabilities; the sensitivity of the member information being communicated to both the credit union and the members; the ease of using the communication method; and the volume of transactions. The risk assessment should include an evaluation of the methodology used to authenticate members. NCUA considers single-factor authentication, as the only control mechanism to authenticate members, to be inadequate for high-risk transactions.

If the risk assessment identifies the credit union providing high-risk Internet-based products and services and single-factor authentication is the only control mechanism, additional controls need to be implemented. Those controls can be multifactor authentication, layered security, or other controls reasonable to mitigate the risk.

The Authentication guidance also addresses the need for credit unions to have monitoring systems which can determine if unauthorized access to computer systems and member accounts has occurred. Policies and procedures should be in place to report unauthorized access to local law enforcement, your NCUA Regional Director, and members, if the analysis of the breach warrants member notification.

Lastly, credit unions need a program to educate members on fraud prevention. Member education is critical to reduce fraud and identify theft. Current member education programs need to be evaluated to determine if additional steps are necessary.

Credit unions which provide Internet based products and services to members need to complete a risk assessment, determine if the authentication methodology is adequate based on the risk assessment, implement additional controls if high-risk Internet-based products and services are provided and single factor authentication is the only control mechanism to authenticate members, implement monitoring systems to determine if unauthorized access occurs, and evaluate member educations program by yearend 2006.

The FFIEC has released frequently asked questions (FAQs) to aid in the implementation of the interagency guidance on Authentication in an Internet Banking Environment. The FAQs (enclosed) are designed to assist credit unions and their technology service providers to conform to the guidance. They provide information on the scope of the guidance, the timeframe for compliance, risk assessments, and other issues.

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

Sincerely,

/s/

JoAnn M. Johnson
Chairman