REGULATORY ALERT

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

DATE: May 2011 **LETTER NO.: 11-RA-03**

TO: All Federally Insured Credit Unions

SUBJ: Security Incidents Prevention and Detection

ENCL: NSA Information Assurance Advisory,
US-CERT Early Warning and Indicator Notice

Dear Board of Directors:

In response to several recent security breaches involving unauthorized access to vendors' systems that might impact federally insured credit unions (FICUs), this risk alert highlights appropriate security incident prevention and detection steps for FICUs to protect and secure their members' information.

FICUs should have robust enterprise risk management practices in place to maintain member data integrity and confidentiality. The components of sound and prudent risk management include risk assessment, risk mitigation and controls, and risk measuring and monitoring. FICUs should perform periodic risk assessments of their information security programs with respect to the prevention and detection of security incidents.

Lack of proper monitoring and control systems allows attackers to gain entry into a target environment through phishing, spear-phishing, drive-by malware injection, and other malicious techniques. Once attackers have entered an environment, they typically use sophisticated tools and techniques to gain access to sensitive data or systems, install a backdoor virus, and exploit system vulnerability. Successful attacks often compromise sensitive member information which may lead to fraud. The increasing sophistication of the tools and techniques attackers use often includes stealth or other means that make their detection more difficult.

We expect FICUs to review carefully the enclosed National Security Agency (NSA) Information Assurance Advisory and the United States Computer Emergency Readiness Team's (US-CERT) Early Warning and Indicator Notice (EWIN). Both are associated with one of the recent events.

The NSA advisory provides detailed recommendations consistent with previously issued NCUA and Federal Financial Institution Examination Council guidance. Proper physical and logical controls should be implemented to restrict and monitor access to sensitive information, systems, and control components. FICUs should ensure that their information security program includes the evaluation and appropriate disposition of the above-mentioned recommendations based upon their environment and risk profile.

The US-CERT EWIN contains a list of domains associated with malicious activity. FICUs should prohibit network traffic -- both inbound and outbound -- within those domains.

US-CERT and the NSA have published notices and alerts containing recommended mitigation strategies relevant to security incidents posted on the Financial and Banking Information Infrastructure Committee (FBIIC) website (www.fbiic.gov). FICUs are encouraged to access them.

If you have any questions regarding this risk alert, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/

Debbie Matz
Chairman

S:\National Issuances\Regulatory Alerts\ Incidents Prevention and Detection\ Regulatory Alert - Security Incidents Prevention and Detection - May 2011.docx

S:\National Issuances\Regulatory Alerts\ Incidents Prevention and Detection\ IAA-28March2011.pdf

S:\National Issuances\Regulatory Alerts\ Incidents Prevention and Detection\ EWIN -11-077-01A UPDATE.pdf