NCUA RISK ALERT

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

DATE: February 2013 RISK ALERT NO.: 13-Risk-01

TO: Federally Insured Credit Unions

SUBJ: Mitigating Distributed Denial-of-Service Attacks

Dear Board of Directors and Chief Executive Officer:

The increasing frequency of cyber-terror attacks on depository institutions heightens the need for credit unions to maintain strong information security protocols. Recent incidents have included distributed denial-of-service (DDoS) attacks, which cause Internet-based service outages by overloading network bandwidth or system resources. DDoS attacks do not directly attempt to steal funds or sensitive personal information, but they may be coupled with such attempts to distract attention and/or disable alerting systems.

Risk Mitigation

This alert identifies appropriate policies and procedures to guard against DDoS attacks. Such attacks are sophisticated, requiring the vigilance of credit unions offering Internet-based financial services. As the goal of DDoS attacks is causing service outages rather than stealing funds or data, typical network security controls – such as Firewalls and Intrusion Detection and Prevention Systems – may offer inadequate protection.

Key strategies for mitigating DDoS risk include:

- Performing risk assessments to identify risks associated with DDoS attacks.
- Ensuring incident response programs include a DDoS attack scenario during testing and address activities before, during, and after an attack.
- Performing ongoing third-party due diligence, in particular on Internet and web-hosting service providers, to identify risks and implement appropriate traffic management policies and controls.

In addition, credit unions should voluntarily file a Suspicious Activity Report (SAR) if an attack impacts Internet service delivery, enables fraud, or compromises member information.

DDoS attacks may also be paired with attempts to steal member funds or data.

Credit unions should employ controls described in the 2011 FFIEC supplement to guidance on *Authentication in an Internet Banking Environment*, and in various recent alerts. (See the Appendix on the final page of this letter.)

General risk mitigation practices for credit unions with an Internet presence include:

- Maintaining strong information security awareness programs for employees and members.
- Utilizing transaction monitoring, verification procedures, and appropriate limits commensurate with the risk of applicable funds transfers.
- Implementing strong controls over computers used to process commercial payments, including but not limited to:
    - Multifactor authentication.
    - Removal of hardware tokens upon session completion.
    - Prohibited or highly filtered use of Internet browsing.
    - Dedicated, corporate-owned systems without administrator privileges.
- Following network and application security best practices with regard to configuring systems, patch management, and security testing.

Threat Monitoring

Appendix A to Part 748 of NCUA's Rules and Regulations requires credit unions to monitor systems to detect actual and attempted attacks on or intrusions into member information systems. NCUA also encourages credit unions to participate in information-sharing organizations, such as industry trade groups and the Financial Services Information Sharing and Analysis Center (FS-ISAC), http://www.fsisac.com. In addition, the United States Computer Emergency Readiness Team (US-CERT), http://www.us-cert.gov, provides information on the methods used to launch attacks and risk mitigation tactics to reduce their impact.

Credit unions significantly affected by DDoS or other cyber-terror attacks should notify their NCUA Regional Office or State Supervisory Authority. When applicable, credit unions must also follow notification procedures outlined in NCUA Rules and Regulations Part 748 Appendix B, *Response Programs for Unauthorized Access to Member Information*.

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

Sincerely,

/s/

Debbie Matz
Chairman

Appendix

NCUA Resources

- Appendix A to Part 748 of NCUA's Rules and Regulations
- Letter to Credit Unions #11-CU-09: Online Member Authentication Guidance Compliance Required by January 2012
- Letter to Credit Unions #05-CU-18: Guidance on Authentication in Internet Banking Environment
- Letter to Credit Unions #02-CU-17: e-Commerce Guide for Credit Unions

Interagency Resources

- FFIEC IT Handbook Booklet: Information Security
- FFIEC IT Handbook Booklet: Outsourcing Technology Services
- OCC Alert #2012-16: Information Security: Distributed Denial of Service Attacks and Customer Account Fraud

Other Resources

- FS-ISAC/US-CERT/FBI: Fraud Alert, Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud
- US-CERT: Technical Information Paper TIP-12-298-01 Website Security
- BITS Financial Services Roundtable (http://www.bits.org): Cyber Attacks: Strategies for Response (membership required)
- Financial Crime Enforcement Network FIN-2011-A016: Account Takeover Activity