Office of Thrift Supervision
Department of the Treasury
Thomas A. Barnes
Deputy Director, Examinations, Supervision, and Consumer Protection
1700 G Street, N.W., Washington, DC 20552 • (202) 906-5650

April 20, 2011

MEMORANDUM FOR: **Chief Executive Officers**

FROM: Thomas A. Barnes, Deputy Director /s/ Thomas A. Barnes
Examinations, Supervision, and Consumer Protection

SUBJECT: Incident Prevention and Detection - Protecting Information Security

This alert highlights the need for thrifts and their technology service providers (TSP) to take steps to ensure their enterprise risk management is sufficiently robust to protect and secure the thrift's own and their customers' information.

Several recent security breaches have highlighted the need for financial institutions and their TSPs to perform periodic risk assessments of their information security programs with respect to the prevention and detection of security incidents. Most security-related incidents occur because of the lack or failures of basic controls that allow attackers to gain entry into a target environment through phishing, spear-phishing, drive-by malware injection, and other techniques. Once attackers have entered an environment, they typically use sophisticated tools and techniques to gain access to sensitive data or systems. Successful attacks often compromise sensitive customer information or create fraud. The increasing sophistication of the tools and techniques attackers use often includes stealth or other means that make their detection more difficult.

The Office of Thrift Supervision (OTS) expects its financial institutions and their TSPs to review carefully the National Security Agency's (NSA) Information Assurance Advisory dated March 28, 2011, and the United States Computer Emergency Readiness Team's (US-CERT) Early Warning and Indicator Notice (EWIN) 11-077-01A Update, both associated with one of the recent events. The NSA Advisory provides detailed recommendations consistent with previously issued OTS and Federal Financial Institutions Examination Council guidance. Access to sensitive information, systems, and control components should be highly restricted and carefully monitored. Financial institutions should ensure that their information security program or that of their TSPs 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. Financial institutions and their TSPs should prohibit network traffic, inbound and outbound, within those domains.

You may direct questions regarding this Alert to Sandra Chan, Director, IT Examinations, at (202) 906-6540.

Attachments: NSA Information Assurance Advisory dated March 28, 2011
US-CERT EWIN 11-077-01A Update