BANKING ALERT

4/8/14

Financial Regulators Issue Statements on ATM Fraud and DDoS Attacks

Financial regulators at the Federal Financial Institutions Examination Council (FFIEC)[i] recently issued two joint statements to financial institutions on the risks associated with cyber-attacks on Automated Teller Machine (ATM) and card authorizations systems and ongoing distributed denial of service attacks on public-facing websites. The statements were not issued in response to any particular threats, but were meant to make banking and other financial institutions aware of ongoing cyber-threat trends.

Cyber-attacks on Financial Institutions' ATM and Card Authorization Systems

FFIEC members are particularly warning of so-called "Unlimited Operations" attacks that seek to gain access to, and alter the settings on, ATM web-based control panels used by small-to medium-size financial institutions. Unlimited Operations are a type of ATM cash-out fraud where criminals access ATM systems and are able to withdraw funds beyond the cash balance in customer accounts or beyond other control limits typically applied to ATM withdrawals. The FFIEC statement cites an instance in which a recent Unlimited Operations attack netted over $40 million by using only 12 debit card accounts. In light of the large-dollar losses that may occur in an Unlimited Operations attack, the FFIEC statement recommends a multi-step risk mitigation program. In addition to adherence to prior guidances on cyber-attack risk management, the FFIEC expects financial institutions to take the following steps, as appropriate:

- Conduct ongoing information security risk assessments;
- Perform security monitoring, prevention, and risk mitigation;;
- Protect against unauthorized access;
- Implement and test controls around critical systems regularly;
- Conduct information security awareness and training programs;
- Test incident response plans; and
- Participate in industry information sharing forums.

Distributed Denial-of-Service (DDoS) Cyber-Attacks

In a second joint statement, FFIEC regulators warned financial institutions of risks associated with continued distributed denial-of-service (DDoS) attacks on public websites. DDoS attacks often cause slow website response times and prevent customers from accessing institutions' public websites. While DDoS attacks are often political, they sometimes serve as diversionary tactics utilized by criminals attempting to commit other types of fraud, including the use of stolen customer or bank employee credentials to initiate fraudulent wire or automated clearinghouse transfers.

The statement indicated that it expects that financial institutions address DDoS readiness as part of ongoing information security and incident response plans. In addition to regulatory requirements and information contained is other FFIEC guidance documents, the FFIEC requires the implementation of the following risk mitigation steps:

- Maintain an ongoing program to assess information security risk that identifies, prioritizes, and assesses the risk to critical systems, including threats to external websites and online accounts;

- Monitor Internet traffic to the institution's website to detect attacks;
- Activate incident response plans and notify service providers, including Internet service providers (ISPs), as appropriate, if the institution suspects that a DDoS attack is occurring. Response plans should include appropriate communication strategies with customers concerning the safety of their accounts;
- Ensure sufficient staffing for the duration of the DDoS attack and consider hiring pre-contracted third-party servicers, as appropriate, that can assist in managing the Internet-based traffic flow. Identify how the institution's ISP can assist in responding to and mitigating an attack;
- Consider sharing information with organizations, such as the Financial Services Information Sharing and Analysis Center and law enforcement because attacks can change rapidly and sharing the information can help institutions to identify and mitigate new threats and tactics; and
- Evaluate any gaps in the institution's response following attacks and in its ongoing risk assessments, and adjust risk management controls accordingly.

For further information on the interpretation or implementation of the FFIEC statements on cyber-attacks on financial institutions' ATM and card authorization systems or DDoS cyber-attacks please contact **Mark D. Belongia** at 312.582.1605 or mbelongia@ralaw.com.

[i] The FFIEC is comprised of the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Association, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.