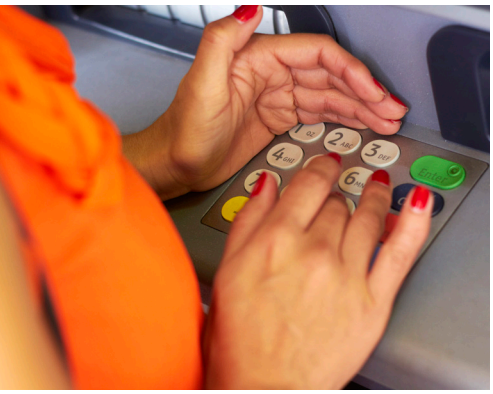

ATM PIN Security Controls

Board oversight is critical for financial, regulatory and contractual reasons.

By Peter Trombley

The financial reason for paying attention to how personal identification numbers are protected at ATMs is in the news every day.

As most directors are aware, ATM fraud is on the increase. A study by FICO Card Alert Service (*http://tinyurl.com/ficocas)* reported that there has been an increase of 546 percent in the number of ATMs compromised in the United States in 2015 compared to 2014. If members lose funds, CUs may have to replace them (even above their bond for a massive cash-out attack).

Boards also need to ensure PINs are protected at their CUs for compliance and contractual reasons.

More Focus on Cybersecurity

All CU boards have a moral obligation and a regulatory duty to protect members' data. Per Appendix A of the National Credit Union Administration's rule 748 (*http://tinyurl.com/ncuasecrule*), the board, or an appropriate committee, is responsible for overseeing the development, approval, implementation and maintenance of the CU's information security program.

Each year the president, with full board approval, must attest that the CU's program equals or exceeds rule 748's standards. Without validating the CU's PIN security controls—and many CUs don't—this attestation cannot be accurately completed.

Additionally, the Federal Financial Institutions Examination Council's new Cybersecurity Assessment Tool (*http://tinyurl.com/ffieccyberassess*) addresses the risk of various electronic delivery channels, including ATMs. If your CU owns ATMs, FFIEC says you have moderate to significant risk exposure. NCUA has already indicated that its examiners will be using this tool and looking closely at payment systems security.

Another key tool is TR-39 (*http://tinyurl.com/ansitr39*), "PIN Security and Key Management Review" from the American National Standards Institute. TR-39 (previously "TG-3") is both a set of standard controls and a method to validate and report compliance with these controls, which meter the security of a member's PIN from the ATM through the debit network to the card-issuing institution.

Contractual Reason

The contractual reason for boards to keep an eye on ATM PIN security arises from the particular ATM network that a CU uses for foreign PIN debit transactions that take place at the ATMs the CU owns. Most networks require their members to meet industry standard security controls and to indemnify other network members for losses caused by a CU that's out of compliance.

Several ATM networks—Pulse, Star and NYCE—have established an exam-based certification for auditors of credit union ATM PIN security. The CTGA (Certified TR-39 Auditor) designation identifies individuals who exhibit a mastery of the standards for securely handling PINs and the encryption keys used to protect them. Typically, CU staff members don't seek this certification for two reasons: It's fairly cost- and time-intensive, and the networks require the ATM auditor to be independent of the operations being audited.

The TR-39 review is a small compliance effort with a big payoff; the onsite review is usually accomplished within a day but can often result in identifying and correcting significant debit compromise risks.

ATMs offer a wonderful convenience to our members, and each CU must make its best effort to ensure that this convenience is safe and secure. In today's environment, boards will want to ensure that the CU is protected financially by being compliant with government rules and industry standards.

CUES Director member Peter Trombley, *CTGA, is chairman of $175 million TCT Federal Credit Union* (www.tctfcu.org*), Ballston Spa, N.Y., and managing director of Bankcard Compliance Group* (www.bankcardcompliance.com*). He has more than 20 years of experience providing information technology and security consulting to financial institutions. Reach him at* peter@bankcardcompliance.

Resources

Read more about FFIEC's Cybersecurity Assessment Tool at *cues.org/0316techtime* and the role of insurance in mitigating cybersecurity risk at *cues.org/0716cybersecurity.* Also read about the 2016 compliance landscape at *cues.org/1115oncompliance.*

"Secure Might Actually Be Insecure" will be a keynote session at Directors Conference (*cues.org/dc*) this December in Maui. Rates increase $400 Oct. 27.