ATM Best Practices and Hardening Checklist

Date: 05/15/25

This checklist is designed to help financial institutions - particularly community banks - implement and verify strong ATM security controls.

1. Physical Security

☐ Install ATMs in well-lit, secure locations with surveillance coverage (CCTV).

☐ Video surveillance footage is retained per policy (typically 90+ days).

☐ Use anti-skimming devices on all card readers.

☐ Inspect ATMs regularly for signs of tampering (false fronts, overlays).

☐ Anchor ATMs securely to prevent theft.

☐ Use high-security locks and limit physical access to technicians.

☐ Maintain an audit log for maintenance and service visits.

☐ Install vibration/shock sensors to detect drilling or cutting attempts.

☐ Use ink dye packs or currency-neutralization systems in case of forced access.

☐ Regularly test physical alarm systems connected to ATMs.

2. Network Security

☐ Use VPNs or private circuits (MPLS, etc.) for ATM-to-host communication—never public internet.

☐ ATM communications are encrypted (e.g., TLS or VPN for IP-based ATMs).

☐ Segment ATM networks from other internal networks (use VLANs or dedicated firewalls).

☐ Enforce IP whitelisting and restrict allowed ports/protocols (e.g., block all except required ports).

☐ Regularly monitor network traffic for anomalies or unauthorized connections.

☐ Ensure remote access (if used) is tightly controlled with MFA and logging.

☐ Use MAC address filtering to restrict which devices can connect to the ATM network.

☐ Perform routine vulnerability scans and penetration tests of ATM network infrastructure.

3. Logical/Software Security

☐ Harden the operating system (disable unused services, remove bloatware).

☐ Apply all relevant OS and application security patches promptly.

☐ Use whitelisting for executable applications (e.g., AppLocker or third-party tools).

☐ Disable all unused USB and serial ports in BIOS and OS.

☐ Enforce strong authentication for administrative access (e.g., smart cards, MFA).

☐ Run antivirus/anti-malware solutions with regular signature updates.

☐ Enable full disk encryption to protect ATM data at rest from theft or unauthorized access.

☐ Use secure boot configurations to prevent bootkits or unauthorized OS loading.

☐ Disable auto-run and script execution to mitigate USB-based attacks.

☐ Remote key loading is encrypted and authenticated.

4. ATM Application Configuration

☐ Ensure the ATM application is locked down and can't be exited to access the OS.
☐ Enable journaling and transaction logging.
☐ Configure alerts for suspicious activity (e.g., repeated failed PINs, physical intrusion alerts).
☐ Remove or disable default passwords and accounts from ATM software.
☐ Use encrypted PIN pad (EPP) and enforce full encryption of cardholder data (PCI DSS compliant).
☐ Ensure ATM software logs are securely stored and transmitted (preferably encrypted).
☐ Implement application-layer integrity monitoring (to detect unauthorized software changes).

5. Access Control & Monitoring

☐ Enforce the principle of least privilege for all ATM service accounts.
☐ Implement role-based access controls and dual control for sensitive operations.
☐ Enable real-time alerting for intrusion, unauthorized access, or tampering.
☐ Maintain comprehensive access and audit logs and review them regularly.
☐ Use centralized SIEM logging for all ATM-related logs and events.
☐ Rotate service credentials regularly and audit service account usage.

6. Vendor & Patch Management

☐ Establish a formal patching process with your ATM vendor for OS and app updates.
☐ Validate updates in a test environment before applying to production.
☐ Ensure third-party vendors follow your institution’s access and security policies.
☐ Require third-party service providers to sign security and confidentiality agreements.
☐ Require vendors to use secure, logged service channels (e.g., jump servers with session recording).
☐ Vendor access to ATMs (remote or onsite) is logged and reviewed.
☐ Establish a review cycle for third-party risk assessments tied to ATM services.

7. Compliance & Risk Management

☐ Conduct regular ATM risk assessments (physical, logical, and operational).
☐ Align ATM security practices with GLBA, FFIEC, PCI DSS, and other applicable frameworks.
☐ Document policies and procedures for ATM maintenance, upgrades, and incident response.
☐ Include ATMs in business continuity and incident response plans.
☐ Include ATM scenarios in tabletop incident response drills.
☐ Perform periodic assessments against PCI PIN Security Requirements and PCI DSS, even if not strictly required.
☐ Maintain documentation of encryption key management procedures.

8. User Education & Awareness

☐ Train frontline staff to recognize and respond to signs of ATM tampering and compromise.
☐ Provide customer education on skimming, shoulder surfing, and suspicious behavior.
☐ Post emergency contact information near ATMs for suspicious activity reporting.
☐ Periodically assess ATM placement and surrounding areas for customer safety risks.
☐ Use screen overlays to warn users about card skimming or suspicious individuals.