STATE OF INDIANA **DEPARTMENT OF FINANCIAL INSTITUTIONS**

30 South Meridian St.
Suite 200
Indianapolis, Indiana
46204-2759
(317) 232-3955
(800) 382-4880
www.in.gov/dfi

Depository Division
Advisory Letter 2025-04
October 14, 2025

To: **All State-Chartered Banks and Credit Unions**
From: **Christopher C. Dietz, Deputy Director – Depository Institutions**
Re: **State-Wide Increase in ATM/ITM Jackpotting Occurrences**

Financial institutions across the state have experienced a recent increase in Automated Teller Machine (ATM) and Interactive Teller Machine (ITM) Jackpotting incidents. These incidents have affected financial institutions of various sizes and geographical locations, and the method of perpetration continues to evolve. The Department is issuing this advisory to increase awareness and provide some industry shared mechanisms to mitigate ATM/ITM intrusion risk. Risk mitigants discussed in this advisory should not be construed as the only mechanisms to mitigate risk nor should this advisory be construed as prescriptive regulatory expectations on ATM/ITM instrusion risk management by the Department.

ATM/ITM Jackpotting is a sophisticated cyber-physical attack where criminals use an ATM and/or ITM to dispense cash without a legitimate transaction. Jackpotting also involves criminals gaining control over an ATM/ITM's system through malware or hardware manipulation to make it dispense all its money, like hitting a "jackpot." Recently, financial institutions have experienced a greater criminal emphasis on accessing ATM/ITM hard drives to dispense cash and possibly to access information stored on the device.

Attack Categories

Criminals use several attacks, including logical attacks, black box attacks, and brutal drive attacks.

- **Logical Attacks**: Involve installing malware via USB or network access to control the ATM's cash dispense.
- **Blackbox Attacks**: Criminals disconnect the ATM/ITM's internal computer and connect their own device to send dispense commands.
- **Brutal Drive Attacks**: Criminals remove the ATM/ITM's hard drive, infect it with malware, and reinstall it to trigger unauthorized cash-outs.

Why It Matters

Jackpotting attacks can drain tens of thousands of dollars in minutes and cause:

- Operational downtime
- Financial loss
- Potential customer PII exposure
- Costly forensic investigations and repairs

Potential Industry Shared Mitigants to Jackpotting Attacks

1. **Physical Security Enhancements**
   - **Rekey ATM Cabinets**: Replace standard locks with tamper-evident seals. Avoid universal keys that are easily purchased online.
   - **Install Alarms and Sirens**: Add tamper visual/auditory deterrents to the ATMs/ITMs.
   - **Surveillance Cameras**: Use cameras to place ATM/ITMs in well-lit, monitored areas.
   - **Power**: Determine if the vendor provides a power disconnect option to disable the ATM/ITM if the top hat alarm is triggered.
   - **Alarm Sensors**: Randomize placement of the alarm sensors.

2. **Software & Firmware Hardening**
   - **Encrypt Hard Drives**: Prevent unauthorized access to data stored on hard drives.
   - **BIOS Whitelisting**: Apply BIOS-level whitelisting to restrict unauthorized hardware and password-protect BIOS settings.
   - **Patching**: Patch operating systems and ATM/ITM software regularly to close known vulnerabilities. Before administering updates, ensure no malware is already present.
   - **Disable Unused USB Ports**: Prevent malware injections via USB and lock down XFS APIs (used to control ATM hardware).

3. **Network & API Protection**
   - **Firewalls**: Configure firewalls, intrusion detection systems, and network segmentation to isolate ATM/ITMs from broader networks.
   - **TLS Encryption**: TLS 1.2 or higher for all ATM/ITM communications to prevent man-in-the-middle attacks.
   - **Endpoint Detection**: Deploy AI-based endpoint security tools to detect and block malware.

4. **Access Control & Monitoring**
   - **Unique Credentials**: Change all default passwords and rotate them regularly.
   - **Multi-Factor Authentication**: If possible, require MFA for all personnel accessing ATM systems.
   - **Monitoring**: Monitor for anomalous dispense patterns (e.g., large withdrawals without card use) and if an ATM/ITM goes offline unexpectedly ensure an alert is triggered to investigate.
   - **System Logs**: Ingest the system logs from the ITM/ATM into a SIEM.

5. **Operational Best Practices**
   - **Training**: Train staff to recognize suspicious behavior and impersonation attempts.
   - **Auditing**: Audit service personnel and verify credentials before granting access.
   - **Penetration Tests**: Conduct penetration testing to identify and fix vulnerabilities.

Summary

To understand and mitigate the risks of ATM/ITM jackpotting, financial institutions must understand the exact implementation method(s) criminals use and how their ATM/ITM units connect and communicate. Limiting physical access to the units is as important as controlling the upstream and downstream network communication avenues. As best practice, hardware and software components that connect to the devices

should be hardened against compromise, monitoring capabilities should be implemented to receive alerts for anomalies, and appropriate response and recovery processes should exist to ensure swift and appropriate action should a compromise occur.