



Community BancService Corporation, Inc.

One Mission. **Community Banks.**

Last year, federal authorities reported an increase in ATM jackpotting schemes targeting community financial institutions throughout four states, including Illinois. In November, twin attacks on a rural Illinois community bank drained its ATMs of more than \$110,000. Prosecutors report the criminals accessed the ATM's interior using specialized keys or tools, and either infected the machine's hard drive with malware or replaced it entirely with a compromised drive containing pre-installed malicious software, all within 90 seconds. This digital takeover enables unlimited withdrawals from the ATM until the currency reserve is completely exhausted throughout the following hours.

During a routine traffic stop on November 11, near Mahomet, Illinois, suspicious travel explanations and identification documents led police to the discovery of ATM components, tools, encrypted communication devices, and nearly \$20,000 in sequentially marked bills from the recent heist. The suspects turned out to be members of a vicious Venezuelan criminal organization. The month-long, four-state crime spree netted the perpetrators nearly \$300,000 from credit unions and community banks.

Despite these arrests, recent jackpotting attacks have been reported throughout Central Illinois. The latest Secret Service data reports a year-over-year increase in ATM logical attacks of more than 200 percent. The National ATM Council has since issued urgent guidelines for biometric access controls for technician panels; real-time transaction monitoring algorithms; and tamper-evident holographic seals on internal components.

CBAI urges its members to take action now before falling victim to the continued threat of jackpotting attacks. Illinois community bankers have begun to take a variety of preventative measures to help secure their ATMs. Jeff Bonnett, president and CEO at Havana National Bank, said his team considered several options before deciding to install steel barriers. "Speed is critically important to these criminals, so slowing them down or drawing more attention to their actions is imperative," said Bonnett. "We want these criminals to take one look at our ATMs and decide the time and effort involved is just too risky."

The bank contacted a local welder, a customer, who designed and installed the steel barriers that are fortified with heavy-duty steel locks. Even using a blow torch, criminals would need at least 30 minutes to cut through their defense.

Bonnett added, "The steel bars and locks cost approximately \$2,000 per ATM. We hope what we have put in place will deter the criminals." With insurance deductibles that would cost the bank upwards of \$20,000 for each ATM hit, the bank feels like their investment is well worth the price.



DBE Offers Solutions to Secure ATMs

CBSC's Preferred Partner for ATM and ITM hardware, DBE, suggests bankers consider implementing the following security measures:

Hard-Disk Encryption – Available through DBE's Encompass Secure Service

TLS 1.2 Encryption – Secure communication between your ATM and host network

Whitelisting – Available through DBE's Encompass Secure Service

DBE secures NCR ATMs they service by locking down BIOS, boot configuration, and internal menus as standard practice.

DBE recommends installing monitored alarms on the top portion of your ATMs and ITMs. Re-keying the top portion is a common action taken. While monitored alarms and re-keying may slow an attack, they do not fully prevent jackpotting on their own.

Stay Ahead of Evolving Threats

Join Paul Cowley, DBE's VP of Technical Support and Logistics, at The DBE Forum on June 11 for an in-depth and in-person session on ATM security and emerging attack methods. RSVP for the Forum [here](#).

For DBE's full ATM security recommendations, visit their [ATM Security Recommendations webpage](#).