TRUSTAGE ATM and ITM risks

Criminals are increasingly turning their attention to the money inside automated teller machines (ATMs) and interactive teller machines (ITMs).

In today's socially distanced world, criminals increasingly are turning their attention to the money inside ATMs and ITMs — and their fraud and physical attacks are causing havoc at an alarming rate.

In fact, three ATM and ITM risk trends have resulted in six- and seven-figure losses for many credit unions over the last 12 – 18 months:

- Unauthorized withdrawals from member accounts using the ITM's self-service feature.
- Jackpotting where the fraudsters cause the machine to dispense cash until it's empty. Fraudsters are using several methods to physically gain access to the inside of the machine.
- Smash-and-grabs where the perpetrators use stolen heavy-duty trucks with chains, construction type vehicles, equipment and even explosives to rip apart the ATM or ITM to gain access to cash canisters.

Fortunately, there are risk mitigation strategies that can significantly minimize the frequency and severity of these losses.

More ATM and ITM risk information

Are machines properly secured and have physical security enhancements in place?+

There are several methods to enhance the physical security of ATMs and ITMs. Some basic physical security measures like changing the lock and universal key to the machine's top hot, installing bollards or steel barriers around and across the machines; securing machines with bolts into concrete; and placing adequate lighting and surveillance coverage are critical. Installing a mercury switch and vibration sensors is also a good idea and can help alert you of lifting, tilting or movement of an ITM or ATM.

Machines located on the outermost drive-thru lane or on an island may be the most vulnerable. Of course, conducting daily inspections of all ATMs and ITMs to uncover tampering can be helpful in minimizing losses. Use this **ATM inspection checklist** as a guide on what to look for.

Do you limit currency amounts, and have you reassessed your replenishment schedules for ATMs and ITMs?+

Reevaluating currency replenishment schedules and limiting cash amounts is a deterrent and a good way to minimize losses. In many cases, it appears the criminals monitor the credit union to identify when the attack would be most lucrative. Varying replenishment schedules and limiting currency amounts are highly advisable.

Are controls in place to minimize fraud associated with unauthorized withdrawals and jackpotting?+

You should consider several mitigation tips to help minimize fraudulent unauthorized transactions:

- Block fallback transactions for the self-service feature on ITMs. Consider completely disabling the self-service feature or at least limit its hours of operation to normal business hours only.
- Ensure ITM withdrawals limits — both single transaction and daily limits — are reasonable to limit the potential exposure.
- Don't allow members to take advances against their line-of-credit loans using the self-service feature.
- Deploy out-of-band authentication using passcodes when members are authenticated with their account number and another piece of information, such as the last four digits of their Social Security number.

To minimize jackpotting risks:

- Replace the lock and equip machines with an alarm. Fraudsters typically access the machine through the top hat.
- Encrypt the machine's hard drive.
- Encrypt the communication between the machine and the acquirer's host system. If a router is used, the communication link between the machine and the router must also be protected.
- Ensure security patches are installed when they're made available.

Review reports daily (ideally in the morning) on the velocity of transactions performed at your ATMs or ITMs to determine normal activity. An increase in velocity may indicate a compromise of member data or cards.

Related resources:

ATM and ITM emerging risks video

https://cunamutual.widen.net/s/gcglwx5kvt/er-outlook---atms_itms