TruStage™

Interactive teller machines (ITMs)

Risk overview

Interactive teller machines (ITMs) are more popular within financial institutions as they can save time, provide member convenience, and drive efficiency. ITMs can serve as a traditional ATM, act as a video assistance teller, or provide self-service options. However, fraudsters and criminals also find ITMs useful and convenient to gain access to money if the proper controls and security are not in place.

An ITM typically uses a combination of touch screens and video technology to offer a virtual version of the in-person banking experience. Members can walk or drive up to the ITM, press begin and conduct transactions – including starting a video conversation with a live member service representative at designated times.

ITMs are a good option for credit unions:

- Because video tellers can be distributed across ITM branches or machines, you can hire fewer people to manage more members.
- The average cost of assisting a member tends to be lower as the locations are independent of where your members are located.
- The ability to reduce physical branch location costs. ITMs are often very useful in situations where physical footprints are small or when the membership you're serving is small and spread out.
- ITMs operate remotely and allow credit unions to expand your hours and serve members who normally have to make a concerted effort to access your full services within the branch.

Authentication tools such as a debit card/PIN or social security number can be compromised either by a shimmer/skimmer installed on the ITM (or ATM) or by obtaining it through other means. Because these transactions are run through core systems; they often have larger withdrawal limits and access to several accounts held by the member. In addition, these fraudulent transactions are often completed during off hours.

ITM functionality

Typical ITM services include:

- Giving cash withdrawals
- Accepting cash deposits and checks
- Paying down loans
- Bill payments
- Opening new checking and savings accounts
- Transfers
- Getting new debit or credit cards
- Facilitating cash advances
- Offering financial advice
- All business account operations
- Money orders and corporate checks

By using electronic signatures and ID verification and authentication, ITMs can perform most any service needed.

Despite the advantages, ITMs are vulnerable to fraud related to checks, card skimming, and account takeovers. In addition, ITMs, like their counterpart ATMs, also can introduce a variety of risks related to physical security, employee safety, and potential compliance risks.

Understanding fraud & ITMs

Fraudsters find ITMs to be very useful in capturing card data by installing shimmers or skimmers or exploiting member's security information by entering the social security number, birthdate and/or account number to gain access to withdraw funds. Authentication tools such as a debit card & PIN or Social Security Number can be compromised either by a shimmer/skimmer installed on the ITM (or ATM) or by obtaining it through other means. Because these transactions are run through core systems; they often have larger withdrawal limits and access to several accounts held by the member.

Fraudulent transactions at ITMs are often completed during off hours for the fraudster to remain relatively unnoticed.

Common ITM fraud

Fraudsters use the self-service feature to withdraw funds from member accounts – primarily using counterfeit debit cards. In some cases, deep insert skimmers are found on ITMs.

A significant number of these incidents have occurred through the self-service option which is available 24/7 to members and can authenticate the member by using their debit card & PIN and/or entering their Social Security Number. When debit cards are used to authenticate a member, a counterfeit debit card may be used to either:

- Perform an ATM withdrawal that is authorized through the card network/ processor, or
- Authenticate the member to gain access to all the member's accounts including checking, savings, HELOCs and other accounts

Skimming

Skimming is one of the most prevalent forms of ITM fraud. Once the card information has been captured from the information stored on your card's magnetic stripe, fraudsters then use this information to create counterfeit cards.

Your credit union should consider the following:

- Install anti-skimming devices or stickers that warn about skimming and/or give a clear vision that tampering may have occurred. For more information on those, I recommend reaching out to your ATM/ITM provider.
- Turn on ATM/ITM transaction monitoring to send emails letting your staff know of high dollar amounts being withdrawn from an ITM in a set timeframe.

Magstripe vs EMV chip authentication

Maintaining support for Magstripe cards is much riskier than chip cards. Magstripe cards can easily be skimmed and duplicated. Allowing bad actors to withdraw money directly from the ITMs with the duplicated cards. Most ITMs can turn off magstripe support.

Fallback transactions occur when a chip-enabled terminal is unable to read the EMV chip and the transaction is then processed by the merchant using the magnetic stripe. Fallback transactions are magnetic stripe or manually key-entered transactions performed with chip cards at chip devices Fallback transactions are considered higher risk transactions, less secure to fraud, and eliminate the chargeback rights for credit unions.

Understanding fraud & ITMs

Fraudsters nationwide are taking advantage of weak security protocols for ITMs/ATMs and attacking the physical terminal by installing malware through the top hat. These attacks – often called jackpotting attacks - attempts to illegitimately dispense cash from an ITM/ATM. Jackpotting events can drain all the cash from the machine. The cash dispensed is not tied to the balance of any one accountholder.

Jackpotting – physical attacks

Fraudsters install malware in a physical attack either by:

- Prying open the ITM top hat using a crowbar or other tool; or
- Obtaining a master key to access the ITM.

In one case, the fraudsters were apprehended and found to be in possession of a Diebold master key for the ITM top hat.

Once the attacker has access to the ITM, the malware is installed using the internal hardware ports. The USB port is the most common infection point; however, older machines using a CD reader have also been abused in the same manner. After the malware is installed, a code is entered, and the money is dispensed. The attacker can command the ITM/ATM to dispense the money immediately or wait until a more opportune time.

Physical malware attacks are typically carried out at night or on the weekends to evade detection. Once infected with malware, the ITM/ATM's middleware is targeted to orchestrate the attack. Middleware is an application programming interface (API) that is used to communicate with the ATM's peripherals (e.g., the PIN pad and money cassettes).

Jackpotting – remote attacks

Malware attacks via the credit union network are more difficult for attackers to carry out; however, remote attacks typically present less risk of being caught. In the remote attacks, fraudsters access the credit union's local network, bypassing existing defenses, which allows them to gain control over the ITM/ATM.

Fraudsters often use phishing emails sent to credit union employees containing attachments infected with malware or links to infected websites. Employees that fall victim to the phishing attack inadvertently provide the necessary employee credentials to hack into the credit union network. Once within the network, fraudsters hack the computers that control the ITM/ATM network and upload the malware which then gives them remote control to the ITMs/ATMs.

Specific times can be set for triggered dispense or fraudsters can arrange for accomplices to wait at the ITMs/ATMs to retrieve the money immediately. Credit unions running machines with old operating software that is no longer supported by the manufacturer are typically more vulnerable to Jackpotting, since these ITMs/ATMs are not receiving important software security patches.

In addition, ATMs/ITMs are targeted through other schemes including fraudsters connecting a device – referred to as a black box – to the ITM/ATM dashboard. The fraudster then uses the black box to send or dispense commands to the cash dispenser. A man-in-the-middle scheme where a device is installed between the ITM/ATM's computer and the network cable connection to the acquirer's host system is also becoming more prevalent. Messages are intercepted and modified specific to the card being used by the fraudster.

Understanding fraud & ITMs

Account takeovers

Fraudsters have launched sophisticated social engineering attacks against members to scam them into providing their login credentials, including two-factor authentication passcodes. Credit unions that allow the use of account number and member information to access their account through the ITM may be more susceptible to account takeovers.

To obtain member account credentials, fraudsters have deployed social engineering scams by:

- calling and spoofing the credit union's phone number and/or texting the member that appears to come from the credit union
- fraudulent text alerts often contain a link to a spoofed website that is made to appear like the credit union's online banking login page

Upon logging into member accounts, the fraudsters typically change their contact information (home & mobile phone numbers and email addresses) through the member profile feature. This allows the fraudsters to intercept any notifications or fraud alerts from the credit union regarding suspicious transactions.

A word of caution! Losses from account takeovers can escalate very quickly as fraudsters can potentially target a very large number of members every day over the course of consecutive days. A credit union could potentially incur thousands of dollars in daily losses.

Account takeover fraud case study
Credit union impact: $575K loss

- Members were scammed into providing their audio response PIN.
- Using the audio response system, the fraudsters changed the PINs
- Fraudsters used account numbers and PINs to access accounts through the ITM.

There are several loss controls to consider to mitigate account takeover risk at ITMs:

- Educate members on the social engineering tactics used by fraudsters to obtain banking credentials.
  - Explain to members that the credit union would never ask for their login credentials including two-factor authentication passcodes.
  - Warn members to not rely on caller ID and instruct them to call the credit union using a reliable phone number if they receive a text or call from someone purporting to be from the credit union.
- Avoid resetting passwords based on a member's phone request.
- Change the settings to the "forgot password" feature so that members cannot use it with an unregistered device.
- Deploy a more secure form of two-factor authentication, such as a token or push notifications to a dedicated app residing on the member's device.
- Deploy a real-time fraud monitoring solution with behavioral analytics that leverages the use of artificial intelligence and machine learning.

Check fraud

Fraudulent deposits may also be a concern for credit unions offering deposits through an ITM. Fraudsters may exploit ITMs by depositing fake checks and withdrawing the funds before the checks are returned.

Consider lowering deposit and frequency limits, along with placing check holds on checks deposited at ITMs, especially on new and low activity accounts. This can help reduce the check fraud risk significantly.

Security considerations for ITMs

- Work with your service provider to keep your operating system and software up to date.
- Ensure real-time monitoring of hardware and software is in place.
- Ensure ATM/ITM hard disks are encrypted to protect from modifications & access.
- Block all fallback transactions at ITMs or ATMs.
- Set low daily dollar limits based on your credit union's risk appetite.
- Eliminate ATM-only cards due to the lack of EMV security.
- Ensure your ITM/ATM vendors utilize detection technology that identifies shimming or any foreign devices such as cameras/camera overlays. Once a foreign device has been detected it would automatically shut down the terminal.

If you are using the ITM self-service option:

- Do not allow easily compromised identification such as members social security number, date of birth or account number as form of authenticating your members.
- If your credit union uses a debit card to authenticate your member; ensure the ITM reads the EMV/chip and if it is not detecting the EMV/chip it does not allow for fallback transactions and declines the transaction.
- Set daily dollar limits for cash withdrawals to one transaction per day.
- Consider setting daily dollar withdrawal limits at the amount you have for ATM withdrawals.
- Implement multi-factor authentication such as a one-time passcode sent to their device before they may proceed with any transaction.
- Consider requiring additional forms of authentication such as an ID that would need to be scanned into the ITM.
- Do not allow access to HELOC accounts.
- Consider limiting hours of operations for self-service options and require members to use the video teller, if available.

- Review reports daily (ideally in the morning) on velocity of transactions performed at the ATM or ITMs to determine if this is normal activity. An increase in velocity may indicate a compromise of member data or cards.
- Ensure all ATMs/ITMs are EMV-enabled.
- Educate members of the risks and to report any signs of tampering or unusual devices on the ATM/ITM terminals.

Understanding physical security & ITMs

ITMs provide more cash holding cassettes increasing currency capacity and providing opportunity for criminals to break into ATM/ITM kiosks, and stand-alone, off-site machines. Their approaches to access the cash contents typically include cutting the fiber optic lines and dismantling cellular alarm antennas; and then:

- using high-powered cutting & grinding tools
- carting away ATMs/ITMs using two-wheel dollies
- pulling ATMs/ITMs from the location using vehicles
- smashing ATMs/ITMs with heavy equipment like trucks with chains, construction-type equipment, and even blow torches or explosives to rip apart the machines.

These smash 'n grab style attacks limit the actual time of attack to sometimes just 2 – 3 minutes for cash canisters to be accessed and/or removed.

Physical security considerations

- Place ATMs/ITMs in well-lit, visible areas with good foot traffic, ideally within a secure building or location.
- Secure stand-alone ATMs/ITMs to the floor and walls to prevent the machine from being rocked from its foundation. There are several methods (e.g., securing with bolts into concrete) to anchor the machines.
- Properly secure the ATM/ITM cabinet from forced entry and have it alarmed. In addition to having the ATM/ITM connected into your alarm system; consider an audio, strobe, and/or flashing light to minimize burglary risk.
- Change out the universal key used to access the machine top hat and ensure appropriate locking mechanisms work to secure access.
- Utilize real-time monitoring of security such as when ATM/ITM goes offline. Going offline can be a sign of tampering with the terminal.
- Install locator devices such as: GPS (satellite), GMS (cellular) and RF (radio frequency).
- Place bollards, concrete barriers, and/or barrier system kits around the ATM/ITM to protect against smash 'n grab burglaries. Machines located on the outermost drive-thru lane or standalone on an island are often the most vulnerable.
- Install guard rail barriers across the ATM/ITM.
- Install a mercury switch which detects lifting or tilting of the machine.
- Install vibration sensors to alert you if there are attempts to drill a hole in an ATM/ITM.
- ATMs/ITMs should provide a burglary resistive unit which is constructed in accordance with Underwriters Laboratories Inc., TL-15 specifications or regulation UL 291 Level I rating for 24 hours use, CEN L, CEN I, CEN II, CEN III and CEN IV. The burglary resistive unit of the machine is the first line of defense against forced entry.
- Use deterrents, such as ink staining and/or GlueFusion, that protects cash contents against unauthorized access and renders it unusable.
- Use area/perimeter protection, such as door contacts, motion detectors, and cameras within the safe area of the ATM/ITM kiosk.
- Conduct simple public awareness campaigns – stickers or screensavers that explain "ATMs/ ITMs are protected." These campaigns are an inexpensive and can be an effective form of deterrent.
- Perform daily machine inspections to ensure the ATM/ITM has not been tampered with, is not obstructed, and that cameras/alarms are functioning properly.

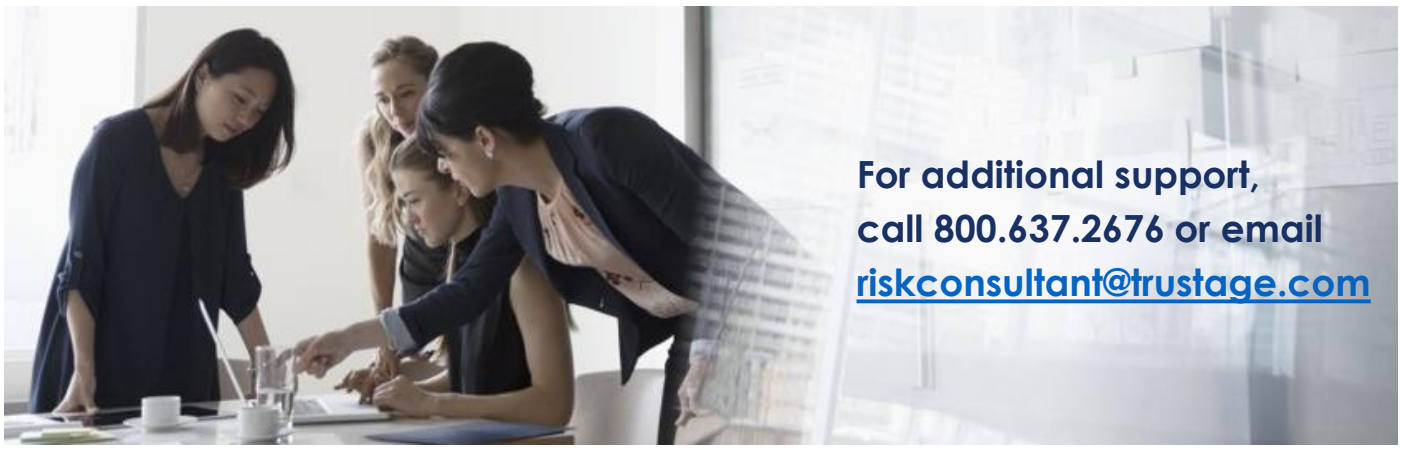
Understanding physical security & ITMs

Potential issues related to ITMs and robbery

ITMs, along with teller cash dispensers/recyclers (TCR/TCD), can help with security or robbery risks as they automate cash handling for tellers. Instead of having to count and manage cash manually, the automated machines provide a more secure system for storing money and dispensing cash.

The machines can act as a robbery deterrent with the correct security and safety features in place.

- Staff should be trained on what to do if there is a robbery at the ITM machine.
- Use an armored car service for currency deliveries, deposits and servicing ATMs/ITMs. Identify courier personnel before relinquishing any currency/deposits. Encourage the armored car service, employees, and ATM service technicians to exercise extreme caution when servicing and/or accessing ATMs. It is recommended that routes and routines should be varied to avoid surveillance and tracking by criminals.
- Maintain a teller cash drawer – other than the ITM - with minimal cash amounts (e.g., $1,000) to be used in the case of a robbery attempt. Instruct staff to always stay calm and obey orders. If the robber requests money that the employee must leave the area for; clearly explain what they need to do to the robber and request permission to do so.
- Consult with TCD, TCR, and ITM manufacturer to determine dispensing options and other security options in the event of a robbery. Place a cash amount limitation on teller or transaction before an override is needed
- Train staff on any selected options that have been implemented.
- Load, unload & service machine(s) under dual control during non-business hours, whenever possible.
- For machines that can, activate the hot button/robbery/duress button that will dispense a predetermined amount of currency. This should be activated to get the robber out of the office as quickly as possible.



TruStage