TruStage™

ATM safeguards

Risk overview & inspection checklist

Automated Teller Machines (ATM) are part of your members' digital culture and are a significant part of the branch of the future. ATMs offer a significant convenience with direct access to cash transactions for both members and non-members alike; however, can also introduce a variety of risks including physical security, employee safety, fraud, malware, and compliance risks.

In today's socially distanced world, criminals increasingly are turning their attention to the money inside automated and interactive teller machines. From a risk perspective, the functionality of an ATM has evolved over time; yet ATMs remain prime targets for criminals and fraudsters looking to score quick cash. And, with more than half million ATMs estimated nationwide, there are ample targets.

Emerging ATM risks

The evolution of ATM risk has exploded with new attack types. Unfortunately, the ATM is a convenient channel for everyone including criminals and fraudsters.

- Fraudsters attack by attaching skimming and shimming devices to ATMs to capture data from the card's magnetic stripe and EMV chips.
- ATM Jackpotting - hackers access and take over the ATM's internal computer, the cash dispenser, and the PIN pad causing the ATM to dispense cash until it is emptied.
- Malware is used to manipulate system controls, inflate account balances and remove daily transactions limits enabling the criminals to withdraw an unlimited amount of cash.
- Fraudsters attack non-EMV enabled ATMs where EMV card readers are not operating correctly due to improper set-up. Credit unions are liable for the chargeback if fraud occurs at their ATM and the ATM is not validating EMV or the credit union's non-EMV card is used at another financial institution's ATM that is EMV enabled.
- Fraudsters are creating counterfeit magnetic stripe cards with non-functioning chips using data compromised in merchant breaches. Fallback transactions occur due to hardware or software issues, a dirty or damaged chip reader, a damaged chip, or due to fraud
- Lawsuits have been initiated against organizations for failing to comply with the ADA's accessible design standards for ATMs and for improper fee disclosures required by Regulation E.
- Criminals use aggressive smash & grab attacks often involving stolen heavy-duty trucks with chains, construction type vehicles, equipment, and even explosives to rip apart an ATM to gain access to cash canisters.
- Third party vendors – e.g., ATM provider, armored car service – lead to losses related to currency transportation, fulfillment, and service.
- Employee and member robbery and physical attacks and safety incidents.

Selecting an ATM location

When selecting an ATM location, confirm that the proposed location complies with any Federal, State, or local laws regarding lighting, cameras, sight lines, ADA compliance, panic buttons, etc.

Additionally, carefully research lighting; traffic patterns; Police protection, and criminal statistics for the proposed location. This type of data is typically obtainable from your local law enforcement agencies, **www.city-data.com** or through other outlets.

Key questions to consider:

- Does the location provide the ability to have adequate surveillance camera to view the surrounding area of the ATM?
- Does the location provide the ability to monitor the ATM by camera or employees during business and after normal business hours?
- Is the location conveniently located so it can be regularly inspected for foreign devise and other security issues?
- Will the ATM be equipped with a panic button?
- Will consumer awareness (security) mirrors be installed?
- Is the location's landscape (e.g., retaining walls, shrubs, trees) maintained on a regular basis to avoid possible hiding areas?
- Is lighting clear of obstruction (e.g., trees block light fixtures)?
- Is the ATM location visible from the street?
- Is parking located near the ATM? Is the parking area free from obstructions?
- Does the traffic flow permit easy access both to and from the ATM?
- Will consumers approach the ATM by walking across the drive-thru or parking traffic?

ATM vestibules / buildings

Providing a safe and secure environment for consumers to perform ATM transactions can be a challenge – even with the use of ATM vestibules and free-standing buildings.

Consider these security features:

- Card mag stripe on door for unlocking door access
- Surveillance cameras
- Emergency phone / panic button
- Video analytics
- Audio analytics
- Security mirrors
- Safe lighting
- Clear site line into the vestibule

Mobile ATMs

Designed to be moved from temporary location to temporary location – such as trade shows, festivals, charity events, sporting events, and other-sponsored activities.

- Develop written policies, procedures, and checklists pertaining to deployment
- Maintain the address and timeframe when the mobile ATM will be utilized
- Determine overnight status and if 24-hour security is necessary
- Control currency storage amounts
- Understand cash replenishment plans
- Consider compliance requirements with the Americans with Disability Act
- Equip the ATM location with security such as a GPS tracking, cameras, mercury switch, and trailer security
- Contact insurance carrier to determine insurance requirements

ATM currency safeguards

Currency transportation

Transportation of currency always represents a risk, especially in higher-crime areas.

If your organization determines the transportation of funds by staff is the only feasible option, the amount of currency transported should not exceed these guidelines:

- One or more employees = $50,000 maximum
- One employee and an armed guard = $100,000 maximum
- Armored car = amounts greater than $100,000

Review the **Currency & vault specifications / storage & transportation guidelines** for additional insights.

Procedures should also include security guidelines for transporting currency:

- Avoid well-established, set patterns or routines
- Vary the time of currency transportation and fulfillment from day-to-day
- Vary the route traveled to/from when possible
- Vary the vehicle used to transport funds
- Do not make any additional stops when transporting currency
- Do not display financial institution moneybags or other containers that indicate the presence of cash

Armored car service

Consider an armored car service for currency deliveries, deposits and servicing ATMs. Insurance protection is typically available through the courier to cover robbery losses while the currency is transported.
The amount of insurance should cover the maximum amount of cash that is being transported.

Although much of the robbery risk is transferred to the armored car service, you should identify courier personnel before relinquishing any currency/deposits and lock delivered currency securely in a safe/vault before in the presence of courier personnel.

It is important to have a copy of the signed contract with your armored car service. Your contract should include but not be limited to:

- Outlined responsibilities and duties of all parties involved
- Specification of confidentiality requirements
- An emergency plan for backup deliveries and/or resumption of service
- Limit of liability amounts for all currency shipments

Encourage your employees, the armored car service and ATM service technicians to exercise extreme caution when servicing and/or accessing ATMs. Also, recommend that they vary routes and routines to avoid surveillance and tracking by criminals.

Use an ATM inspection checklist to assist your organization with performing daily ATM inspections and making necessary corrective actions.

ATM security

Smash and grab style attacks of ATMs have escalated in recent years. This has limited the actual time of attack to sometimes just 2 – 3 minutes for cash supplies to be accessed.

- Secure stand-alone ATMs 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 ATMs.
- Properly secure the ATM cabinet from forced entry and have it alarmed. In addition to having the ATM connected into your alarm system; consider an audio, strobe, and/or flashing light to minimize burglary risk.
- Install locator devices such as: GPS (satellite), GMS (cellular) and RF (radio frequency).
- Place bollards or concrete barriers around the ATM to protect against smash and grab burglaries. ATMs located on the outermost drive-thru lane or standalone on an island are often the most vulnerable.
- Install ATM guard rail barriers across the ATM.
- Install a mercury switch which detects lifting or tilting of the machine.
- Install vibration sensors to alert you if someone attempts to drill a hole in an ATM.
- Conduct simple public awareness campaigns – stickers or ATM screensavers - that explain "our ATMs are protected." These campaigns are an inexpensive and effective form of deterrent.
- Ink staining protects valuables against unauthorized access to its contents by rendering it unusable by marking all the cash as stolen by the degradation agent when an attempted attack on the system is detected.
- Use deterrents, such as ink staining and/or GlueFusion, that protects cash contents against unauthorized access and renders it unusable.

ATM alarm & vault security

- ATMs 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 ATM is the first line of defense against forced entry; however, this physical protection may not provide adequate degree of protection.
- Based upon dollar exposure, electronic alarm protection should be provided. All off-premise ATMs should be electronically protected.
- Install these alarm components on the burglary resistive chest:
  - Door contact, heat sensor & sound detector, vibration sensor, or seismic detector.
  - Low-grade or high-grade line security
  - Audio alarm (sirens) and strobe lights
  - At least 48 hours of standby power
- Use area/perimeter protection, such as door contacts, motion detectors, and cameras within the safe area of the ATM kiosk.

Educate consumers to protect themselves at an ATM

- Remain aware of your surroundings, particularly at night. If you observe or sense suspicious person or circumstances, do not use the machine at that time.
- Prepare your transaction before you approach to minimize time spent at the ATM. Fumbling for your card in front of the ATM makes you vulnerable and takes your attention away from your surroundings.
- If an ATM is hidden from public view (including overgrown landscaping), poorly lit, or ATM lights are not working; don't use it and go to another ATM.
- Avoid using ATMs at night or take a companion with you. Park as close as possible to the ATM. When you have completed your transaction, leave the ATM as quickly as possible.
- If anyone or anything seems suspicious, cancel the transaction and leave immediately. Do not accept assistance from strangers when using an ATM.
- Do not count or visually display cash; instead, pocket it immediately when you complete the transaction, and take your card and receipt. Verify the cash when safe.
- If anyone follows you after making an ATM transaction, go immediately to a crowded, well-lit area and call the police.
- If you are involved in a robbery situation while using the ATM, do not resist. Give the money to the suspect immediately. Contact the police when safe to do so.

Looking for additional insights?

- Access the **Business Protection Resource Center** (User ID & password required) for exclusive risk resources to assist with your loss control efforts.
- If you'd like to discuss this risk in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at **riskconsultant@trustage.com** or at **800.637.2676**.

- Do not use ATMs that appear to be tampered with. Visually review ATMs looking for out of place items like skimmers, shimmers, decals/stickers, or signs of glue.
- Protect your PIN and the privacy of your transaction by shielding the keypad while standing close to the ATM to prevent others behind you from observing your transaction detail.
- Always check your ATM receipt against your statements to identify any unauthorized transactions.
- Immediately report a lost or stolen ATM, debit, or credit card to your financial institution.

TruStage™

ATM inspection checklist

ATM location: **Date:**

Inspected by: **Photographs attached:** ☐ Yes ☐ No

Security - *Evaluate lighting features at night when possible*			
Lights	☐ Operational	☐ Bulbs need replacing	
Landscaping	☐ Free of obstructions	☐ Trees/shrubs need pruning	
Parking lot lights	☐ Operational	☐ Bulbs need replacing	
Surveillance cameras	☐ Working properly	☐ Not functioning properly	
	☐ Correct date & time	☐ Incorrect date & time	
Kiosk door lock	☐ Operational	☐ Not operational	☐ N/A
Alarms	☐ Operational	☐ Not operational	
Power source (if accessible)	☐ Connected	☐ Re-routed	
Top hat	☐ Signs of tampering	☐ No signs of tampering	☐ N/A
ATM decals	☐ Signs of tampering	☐ Hole found underneath	☐ N/A
Description of alarm components not working properly			

Foreign devices			
Skimming/Shimming device	☐ Non-existent	☐ Found attached to ATM	
**To check for shimming devices, use a non-active card and insert into the card reader and (if applicable) the kiosk door card swipe. If there is friction or it is difficult to remove, inspect further.*			
Tape/Glue residue	☐ Non-existent	☐ Found on ATM	
Foreign stickers/decals	☐ Non-existent	☐ Found on ATM	
PIN capture micro-camera	☐ No evidence	☐ Evidence found on ATM	
**Typically located on the leaflet / envelope holder; above the left / right of PIN pad, including light fixture, security mirror, and canopy.*			
PIN-pad overlay	☐ Non-existent	☐ Found on ATM	
Card-trapping device	☐ Non-existent	☐ Found on ATM	
Cash-trapping device	☐ Non-existent	☐ Found on ATM	

ADA requirements – ATMs *Test voice guidance features with ear plugs or earphones*			
Voice guidance	☐ Operational	☐ Not operational	
Voice guidance/volume controls	☐ Operational	☐ Not operational	
Speech interrupt/repeat feature	☐ Operational	☐ Not operational	
Tactile symbols on function keys	☐ Good condition	☐ Deteriorating	
Enter/proceed key	☐ Good condition	☐ Deteriorating	Raised circle
Clear/correct key	☐ Good condition	☐ Deteriorating	Raised left arrow
Cancel key	☐ Good condition	☐ Deteriorating	Raised letter "x"
Braille instruction plate/decal	☐ Intact and legible	☐ Missing	
Screen goes blank (privacy) when voice guidance is activated	☐ Operational	☐ Not operational	

ATM inspection checklist (page 2)

ATM location: **Date:**

Inspected by: **Photographs attached:** ☐ Yes ☐ No

ADA requirements – ATM approach (building code)

Detectable warnings, such as a curb ramp to a sidewalk leading to and from an ATM and/or truncated and directional texture domes, should be in place to indicate transitions to potentially hazardous areas. Credit unions should comply with the related provisions of the **2010 ADA Standards for Accessible Design** – sections 303 (Changes in Level), 406 (Curb Ramps), and 705 (Detectable Warning). Credit unions should also comply with any applicable state law requirements.

Detectable warnings	☐ Exist	☐ Non-existent
Detectable warnings/truncation domes/directional texture	☐ Exist	☐ Non-existent

Regulation E requirements – ATMs *Test ATMs with an ATM and/or debit card not issued by the credit union*

Fee disclaimer	☐ Appears on screen	☐ Does not appear on screen
Fee amount/disclaimer	☐ Correct	☐ Not correct
Transaction cancel to avoid fee	☐ Operational	☐ Not operational
Receipt function	☐ Good, working condition	☐ Not working correctly
Receipt ink	☐ Legible/good condition	☐ Needs replacing
Screen goes blank when voice guidance is activated	☐ Operational	☐ Not operational

Regulation CC requirements – Deposit-accepting ATMs only

Funds availability disclosure	☐ Intact and legible	☐ Missing or non-legible

Additional concerns

Corrective action overview

Corrective actions ☐ Not applicable ☐ Suggested ☐ Law enforcement notified

Corrective actions to be taken

Issue(s) resolved ☐ Yes ☐ No **Date resolved:**

Supporting resolution documentation