TruStage®

Risk & Compliance Solutions | Webinar

ITMs & ATMs:
A Criminal's Money Chest

Convenient channels provide ample targets for fraudsters to score quick cash

Today's panelists

Michael Petrone
TruStage™
Risk Consultant
Maine

Becky Garton
TruStage™
Risk Consultant
Wisconsin

ATMs and ITMs are a significant part of the branch of the future.

They offer a significant convenience; however, can also introduce a variety of risks including physical security, employee safety, fraud, malware, and compliance risks.

Risk evolution

1967 — ATM introduction

Robbery • embezzlement • liability • property damage

1991 — Robberies

Attacking technicians & causing machine malfunction.

Empty envelope deposits.

1994 — Funds availability

Fee disclosures required.

Card fraud takes off.

2008 — Skimming

More losses & controls

Hidden cameras • keystroke loggers

2010 — ADA compliance

Accessibility • keyboard requirements • screen clearing/earphones

2014 — Vendor due diligence

More reliance on vendor providers.

2016 — New requirements

ADA truncated approaches • EMV-enabled machines

Shimmers appear. Malware.

Smash 'n grabs • vendor impersonation • jackpotting

2020's — Off-premises ATMs

Windows vulnerabilities • Bluetooth skimmers

ATM transaction reversal fraud

ITM fraud

Common risks & threats – ITMs | ATMs

Skimming & shimming

Jackpotting & malware

Compliance & litigation

Vendors & third parties

Smash & grabs

Employee & member safety

fraud

security

TruStage®

ITM fraud

ITM fraud risks

Traditional ATM

- Use of counterfeit debit card
- Skimming/shimming risk

Video assistance teller

- Minimal risk
- Be aware of deepfakes and use proper forms of identification that can be scanned into the ITM

Self-service option

- Most risky
- Available 24/7
- Using easily identifiable information that can be compromised
- Using debit card to authenticate member-counterfeit cards easily used and created by skimmers or shimmers

ITM fraud – unauthorized withdrawals from member accounts

What's happening?

- Fraudsters target the ITM's self-service feature during non-business hours (late night over weekends)
- Access member accounts using counterfeit debit cards at ITMs
- Many found deep insert skimmers on their machines
- Others had fraudsters access member accounts using an alternate authentication allowed by the ITM – such as a combination of account number plus a SSN or date of birth
- In some cases, fraudsters took advances against member home-equity line-of-credit (HELOC) loans at the ITMs
- Mid six- and seven-figure losses are common

ITM fraud risk mitigation

In general

- Block all fallback transactions at ITMs and ATMs
- Set reasonable daily withdrawal limits
- Use skimming/shimming detection technology
- Conduct daily inspections of all ITMs/ATMs – including opening to inspect for deep shimmers
    - If foreign device or tampering is detected – machine should automatically shut down
- Ensure all ITMs and ATMs are EMV-enabled
- Educate members of risk at ITM/ATMs – report any signs of tampering

ITM self-service option:

- Avoid using easily compromised identification to access accounts (i.e.: SSN, DOB, account number)
    - Implement one-time passcodes sent to member devices before proceeding with transaction access
- If a debit card is used to authenticate members, ensure ITM reads the EMV chip, if it is not detected decline the transaction
    - Do not allow fallback transactions
- Set reasonable daily withdrawal limits
    - Single transaction and daily limits
- Do not allow access to line of credit accounts
- Limit hours of operations to normal business hours for self-service option and require members to use video teller if available. Machines can function as ATM during nonbusiness hours

ITM fraud case studies

Credit union A

- **Date of loss**: March 24, 2023
- **Members affected**: 197
- **Total loss**: $1,747,785
- **Loss per member**: $8,872
- Withdrawals occurred over a 4-hour period using the self-service feature
- Multiple individual member losses over $50,000

Credit union B

- **Date of loss**: March 4, 2024
- **Members affected**: 302
- **Total loss**: $393,990
- **Loss per member**: $1,305
- Withdrawals occurred over a 6-hour period using the self-service feature

The disparity in losses:

- Both credit unions had a single withdrawal limit of $2,500 but Credit Union A did not have a daily limit – fraudsters made multiple $2,500 withdrawals from a single member's account
- Credit Union A allowed members to take advances against line-of-credit loans (e.g., HELOCs) using the self-service feature while Credit Union B did not
- Credit Union A: Fraudsters took advances against member HELOCs to fund the withdrawals

Anything new in relation to risks associated with skimmers or shimmers?

Trending:

- Targeting/disabling the contactless technology
- Installing skimmer on pay at pump
- The fraudster placed a sticker over the contactless technology, making it appear, out of order
- The member then inserts their card, where the fraudster has placed a skimming device

→| Critical to inspect your ATMs & ITMs daily

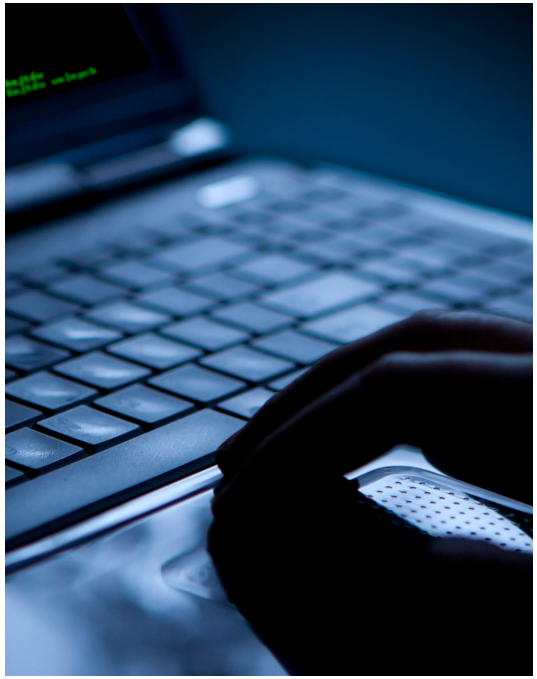
TruStage®

ITM/ATM jackpotting

ITM/ATM jackpotting – causes machine to dispense cash

What's happening?

- Most common: fraudster **infects the machine with malware**. Usually by inserting a flash drive containing malware into the USB port – simply by accessing the ATM/ITM top hat
- Fraudsters connect a **black box**, usually a laptop, directly to the ATM dispenser to send commands to the machine to disburse cash until its empty
- **Man-in-the-middle attack**. Fraudsters install a device between the ATM's computer and the network cable connection to the acquirer's host system. Requires the fraudsters to insert any card - like a gift card or a stolen card – and messages are intercepted and modified



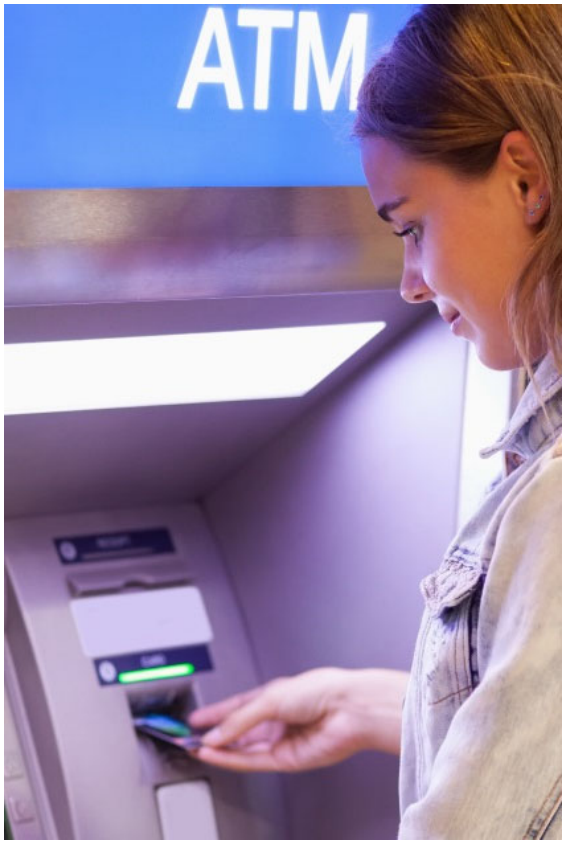
Recent RISK Alerts:

- 4/1/2025 – Loss trends continue to evolve; Implement loss controls to minimize risk (Warning)
- 12/9/2024 – Emerging risks and large losses impacting credit unions nationwide (Warning)
- 10/24/2024 – Fraudsters hit the jackpot with ATM attacks (Watch)
- 11/14/2023 – ATM jackpotting surfaces with black box attacks (Watch)

ITM/ATM jackpotting – causes machine to dispense cash

Mitigation tips

- Work with ATM/ITM vendor
- Replace the ATM/ITM top hat lock and equipping it with an alarm is critical - use an audible alarm to startle the criminal and get them to flee
- 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 the ATM/ITM operating system is supported
- Always ensure security patches are installed when they're made available
- Send a technician to any ATM/ITM that has been offline for at least 5 minutes
- Frequent inspections
- Conduct daily machine inspections



Physical access

- Fraudsters may dress as an ATM technician and physically access the ATM
- Opens top hat with a generic key purchased online or drills hole (about the size of a golf ball) near the PIN pad to gain access (covers the hole with decal)
- Inserts flash drive containing malware to the ATM's USB port or connects black box to the ATM's dispenser
- Fraudster issues command to ATM to dispense cash
- Money mules are used to collect the cash

Another is the MiTM jackpotting attacks:

- Fraudster installs device between the ATM's computer and network cable connection
- Fraudster intercepts and modifies messages from the acquirer's host system for each card transaction – such as, the acquirer sends a decline message that is modified to approve

TruStage®

Smash & grabs

Smash & grabs

A resurgence in ATM/ITM burglaries where criminals use a blow torch or other forced entry to open the machine's money chest or steal it altogether.

Physical security devices:

- Bollards/Concrete barriers
- Barrier system kit
- Sufficient lighting
- Anchor with several specialized bolts and washers
- Strobe light
- External siren or audible alarm

Trending:

Ripping the safe door off by putting tow hook in money slot

- Safe slot reinforcement kit retrofitting current machines
- Security gate
- Security gate alarm - tamper, heat, seismic
- External siren or audible alarm

Emerging risk

Importance of location selection

- Does the location provide the ability to have adequate surveillance camera to view the surrounding area of the ATM?
- Landscape or other obstructions
- Lighting
- Traffic patterns
- Police protection
- Criminal statistics


What are other key security features?

Top things to consider

Alarm is on the ITM/ATM itself

- Door
- Heat
- Seismic
- Tilt
- Line security redundancy for backup (Cellular, Radio Frequency Internet Protocol Digital Dialer)
- Back up / Standby power for alarm system

Machines designed for 24-hour use

- UL 291 Level 1 or 2, CEN L / CEN I, CEN II / CEN IV
- Some are designed for lobby use and the currency must be removed during non-business hours.

Additional security features

- GPS on machine and/or cassettes
- Dye/Ink staining
- Glue fusion

How should we handle servicing ITMs and ATMs?

Currency transportation & servicing tips

- Armored car service
  - Outlined responsibilities and duties
  - Specification of confidentiality requirements
  - Emergency plan for backup deliveries and/or resumption of service
  - Limit of liability amounts for all currency shipments
- Currency transported by employees should not exceed $50,000
- Transport currency in nondescript bag
- Alter time in addition to varying days, routes and routines


We have a mobile branch with ITM/ATMs…
are there any special considerations?

Things to consider – mobile ATMs

- 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

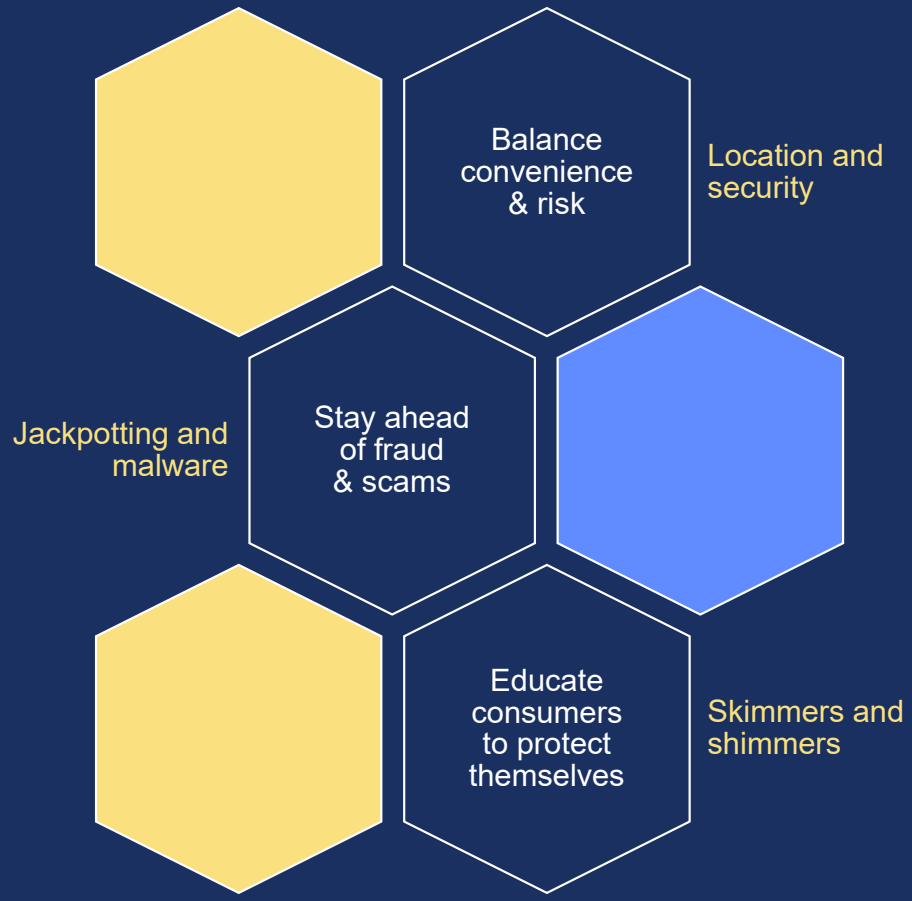

We’ve had a few member concerns…
what suggestions do you have?

Member education

- Be aware of your surroundings. If you sense suspicious persons or circumstances, you most likely want to choose a different ATM
- Visually inspect the ATM for possible tampering
- Avoid visually displaying money received from the ATM and immediately put your money away
- Keep vehicle doors locked, and passenger windows rolled up when at a drive-up ATM
- Choose gas pumps which are closest to the station or retail store rather than those that are out-of-sight or in areas with little traffic
- Take your receipts or transaction records with you following your transaction

Wrap-up

ITM & ATM risks



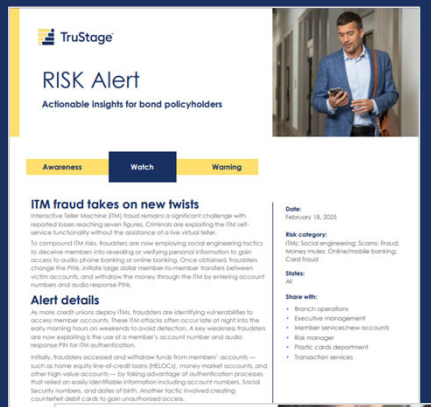
Risk resources

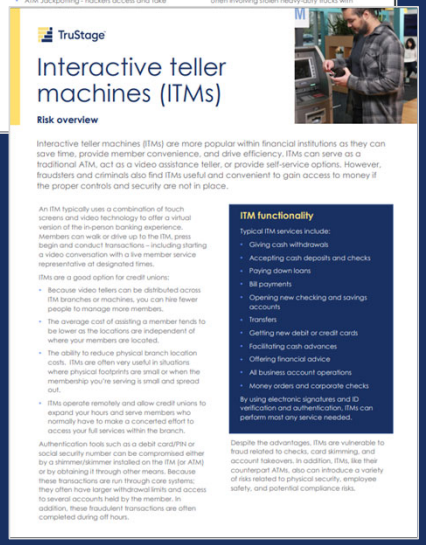
Business Protection Resource Center
www.trustage.com/bprc

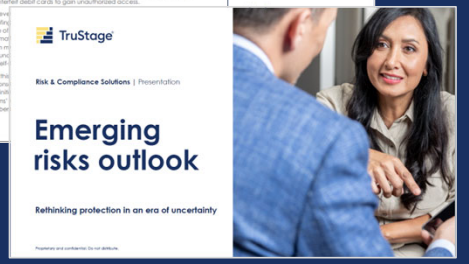
- RISK Alerts – warning | watch | awareness
- Loss prevention library
  - risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

"Great information, excellent format. Presenters were engaging and knowledgeable in their respective fields."

Executive Vice President - $3B credit union







Related links & resources you may find helpful

Business Protection Resource Center @ www.trustage.com/bprc

- RISK Alerts Library
- Loss Prevention Library
- Need access to Resource Center or not receiving Alerts

  >>> step-by-step instructions

"I appreciate that RISK Alerts, articles, and resources are included. It makes it easy to access and extremely efficient."

Risk Manager - $1.1B credit union

"You all make it very easy to keep up with the latest technology and risk involved."

Director of Fraud Prevention - $2.5B credit union

Specific Risk Overviews

- ATM safeguards: risk overview & inspection checklist
- Interactive teller machines (ITMs) risk overview
- Branch of the future risk overview
- Protecting your transactions member guide
- Member tips: protecting your identity & money
- Emerging Risks Outlook

***UserID & Password required**

Contact us

800.637.2676

- riskconsultant@trustage.com
- Ask a risk manager interactive form
- Schedule a 1:1 risk consultation
- Report a risk or scam

TruStage®

Thank you.

Contact
riskconsultant@trustage.com
800.637.2676