

Interactive Teller Machine (ITM)

ATM vs ITM

It is important to understand the key differences between the automated teller machine (ATM) and interactive teller machine (ITM). Though they seem to be quite the same at first glance, the two types of teller machines differ most prominently regarding the accountholder's user experience.

The fundamental purpose of ATMs is to dispense cash, accept cash deposits, and occasionally process simple banking transactions, such as balance transfers. ATMs typically consist of a screen, a card reader, a keypad, a cash dispenser, and a printer. ATMs have a simple computer interface, allowing transactions to be both independent of a branch and without a teller.

ITMs allow the accountholder to speak to a Video Teller or take advantage of the machine's 24/7 ATM functionality. With many ITMs dependent on core support, when talking to the video teller, you may be able to:

- Enjoy extended member service hours
- Authentication with or without a card
- Deposit or cash a check in real time
 - Instant 'on-us' check cashing
 - Deposits to multiple accounts in one transaction
- Receive exact change – including coins
- Make a loan payment
- Make transfers to another account
- Advice and assistance from a live person
- Bill payments
- Currency Transaction Reporting (CTR)
- Office of Foreign Asset Control (OFAC)
- And more!

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.

As technology continues to advance, so do the methods used by criminals to commit fraud. One area where this is particularly evident is with Automated Teller Machines (ATMs) and Interactive Teller Machines (ITMs).

Protect Against Fraud

ITMs have made banking easier for many people, but they also present opportunities for fraudsters to steal personal and financial information. It is important for financial institutions to keep this in mind when configuring their ITMs and weighing the pros and cons between security and convenience.

When you get a new tool with new feature sets, you get excited about the new features you can provide for your accountholders. Just remember, that with new tools, comes new associated risk.

Many financial institutions use ITMs to try to minimize the use of tellers. Because they are thinking about how this machine could replace the teller, they believe that the machine should be able to do all things a branch teller can do. An example of this would be, letting your members withdraw \$5,000 per day through ATM/ITMs. Most members don't require that amount of cash to be withdrawn outside of a couple of times a year. Because of that, does it make sense for your credit union to take such a risk if bad actors were to skim 50 cards and steal \$250,000? I highly recommend thinking through your limits and options to decide what is best for your credit union.

ITMs that offer video tellers give credit unions lots of options to avoid fraud. Limits can be set to call a teller to verify high transaction dollar amounts. So instead of freely giving access to \$5,000 with no supervision, the member could request that dollar amount, which instantly calls a teller for verification. After the teller verifies the member, the money can be withdrawn. This can reduce the risk associated with having a high withdrawal allowance and give your member some freedom to access a large amount of cash from your ITMs.

Fraud Controls

- For both ATM and ITMs only allow authentication using the “chip” or “tap and go”, decline all fallback transactions. The magstripe on cards can easily be skimmed and duplicated, allowing bad actors to withdraw money directly from ATMs and ITMs with the duplicated cards. Most ITM/ATMs

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.

can turn off magstripe support. Contact your card processor to put a strategy in place to only allow “chip” and “tap and go” for all ATMs and POS (Point of Sale) transactions. You invested in chip technology for your cardholders (and “tap and go” at many financial institutions) – defeat the counterfeiters – USE IT!

- Limit ATM/ITM debit card withdrawal transactions to \$500 daily.

ITM Authentication

Implement additional authentication to use the ITM, such as the following functions:

- Deposits
- Withdrawals more than \$500
- Check Cashing
- Transfers
- Payments
- Non-Member Check Cashing
- Require the accountholder see and speak with a live remote teller and present their driver’s license in addition to their debit card.
- Use a palm vein biometric authentication scanner
 - Offers members a highly-secure way to access their accounts.
 - Palm scanners do not retain an image of your palm or fingerprints, but rather use the unique vein patterns and blood flow in your hand to identify you. The intricate vein patterns in your hand are so unique, that this type of authentication is considered more accurate than using fingerprints and faster than an iris scan.

In conclusion, while ATMs and ITMs offer convenience and accessibility, they also present opportunities for fraudsters to exploit your financial institution. By staying vigilant and following these tips, you can protect your accountholders from becoming a victim of ATM and ITM fraud.

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.