Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Interactive Teller Machine (ITM) Fraud

SUMMARY

ITMs have made banking easier for many people, but they also present additional transaction risk compared to traditional Automated Teller Machines (ATMs). It is important for financial institutions to keep this in mind when configuring their ITMs and weighing the pros and cons between risk management and convenience.

Anytime you are adding a new product or service to your financial institution, it is crucial that you consider the added risks that you may be taking on. Features that may be well-intended as convenient or beneficial to accountholders are often exploited by bad actors.

DETAILS

Many financial institutions use ITMs to try to minimize the number of employees needed to operate a branch. Because they are thinking about how this machine could replace the teller, they believe the machine should be able to do all the things a branch teller can do. An example of this would be allowing your members to 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 Most members don't require that amount of cash to be withdrawn outside of a couple of times a year.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?

ITMs that offer video tellers give credit unions many options to avoid fraud. Some ITM providers may allow financial institutions to set limits that require teller intervention for higher-risk transactions. 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 After the teller verifies the member, the money can be withdrawn.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 still give your member some freedom to access a large amount of cash from your ITMs.

MITIGATION STEPS

- For both ATM and ITMs, only allow authentication using the **chip** or **tap and go** methods; decline all fallback transactions. (View previous Risk Alert on Magstripe Fallback)

    - The magstripe on cards can easily be skimmed and duplicated. If fallback is not declined, bad actors can withdraw money directly from ATMs and ITMs with counterfeited cards.
    - Most ITM/ATMs can turn off magstripe support. Contact your ATM/ITM provider and/or card processor to put a strategy in place to only allow **chip** and **tap and go** for all ATM and Point of Sale (POS) transactions.
    - You invested in chip technology for your cardholders (and **tap and go** at many financial institutions) – so defeat the counterfeiters — **USE IT!**
- Limit ATM/ITM debit card withdrawal transactions to **$500 daily** when a video teller is not used.

ITM Authentication

Implement additional authentication layers (beyond PIN alone) to use the ITM for transactions with higher risk, such as the following functions:

- Deposits
- Withdrawals over $500
- Check cashing
- Transfers
- Payments
- Non-member check cashing

Additional authentication options include:

- Require the accountholder to see and speak with a live teller and present their government-issued identification in addition to their debit card.
- Send an authentication code to their phone (the accountholder would have their phone; a fraudster likely would not).
- Using a palm vein biometric authentication scanner:
    - Offers members a highly secure way to access their accounts.
    - Does not retain an image of your palm or fingerprints, but rather uses 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 victims of ATM and ITM fraud.

RISK MITIGATION RESOURCES

- Sign up for our **Let's Talk Fraud** quarterly webinars
- View additional risk resources

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net


Allied Insights
LEARN MORE
Forward-thinking content and original insights into the markets you serve, to help you grow, protect and evolve your business.


Stay Informed
SUBSCRIBE
Sign-up for our newsletters to receive expert education and insights on top-of-mind industry topics and receive resources coming to your inbox.

LinkedIn