Cardless ATM Fraud - What Your Bank Can Do

cyber security risk management ATM

Summary: Bank features and criminal ingenuity are in an evolutionary arm's race, so it should surprise no one that criminals have figured out a way to turn ATM cardless technology to their advantage. We provide tips for your bank to stay safe.

WalletHub did an online survey of winter travel trends and found the following interesting tidbits: 64% of people said they plan to travel away from home this winter, 45% said you can find better travel deals in the winter than the summer, 40% who did not plan to travel this winter said it was because they could not afford it and 37% said travel is worth going into debt. Given winter rolls on through February, you still have some time.

In the banking world, some might say customers have cooled down on ATM usage. We think that is premature, as cardless ATM withdrawal has become a mainstay of mobile banking these days. It keeps technology types engaged and allows customers to skip the card and use an access code and PIN to withdraw cash. It's also a way to quash skimming.

Because there's no physical card, thieves can't skim data. However, cardless withdrawal has its own fraud problems. Criminals can add their own phones to accounts and turn the nearest ATM into a personal jackpot. Better still, cardless withdrawals can be as high as $3,000. That is a big increase over daily maximums between $300 and $600 for standard ATM withdrawals.

Bank features and criminal ingenuity are in an evolutionary arm's race, so it should surprise no one that criminals have figured out a way to turn cardless technology to their advantage.

There's no silver bullet for fraud-proofing cardless ATM withdrawal, but a variety of strategies can help your bank.

Beefing up the security around how banks validate new users and new mobile devices lies at the heart of many of those strategies. Any time a customer adds a new mobile phone number, an alert should go out to all the other phones and computers listed on that account. This gives customers a heads up when a scammer takes the first step in infiltrating an account.

Banks could also restrict how much money a customer can withdraw using a newly added mobile phone number, to reduce the damage a thief can do.

Adding steps to verify a user's identify when a customer adds a new mobile phone number is another good idea, as is limiting customers to a single mobile number. After a user registers that phone with the bank, the bank could verify the number by calling the customer and asking for a texted selfie and photo of the customer's driver's license. Just asking for a username and password isn't enough.

Once a mobile phone is registered with the bank, customers might need to supply a pass phrase or code every time they communicate with the bank. The bank could require that anyone who withdraws money use the registered phone to scan a dynamically generated QR code on the ATM.

Digital identity solutions are more expensive than the other options, but customers seem to like them and your bank can also cross-reference data and pinpoint suspicious activity without creating friction for legitimate

customers.

OUTSOURCED PROFITABILITY SOLUTION FOR YOU

ProfitIntel is an outsourced relationship profitability solution that combines a powerful pricing model with full-time consulting support. Contact us today for more information.