PINNACLE BANK

ATM & Debit Card Safety – Card Skimmers

Debit and ATM card fraud is on the rise. Please take extra precautions to protect your card and your account. Monitor your transactions frequently and report suspicious activity immediately.

Ways To Prevent Fraudulent ATM/Debit Card Activity:

Protect Your Physical Card

- ✓ Always keep your ATM/debit card in a secure place.
- ✓ Never lend your card to anyone, including friends or family.
- ✓ Report a lost or stolen card immediately so it can be deactivated.

Monitor Your Account Frequently

- ✓ Consumer clients are encouraged to take advantage of the Pinnacle Bank mobile banking application ***card controls*** feature. At any point you can turn your card on/off, set limits on transaction amounts, only authorize transactions in specific regions and specific transaction types (such as retail or online).
- ✓ Business clients are encouraged to download the SecurLOCK mobile app. At any point you can turn your card on/off, set limits on transaction amounts, only authorize transactions in specific regions and specific transaction types (such as retail or online).
- ✓ Frequently monitor account activity, if you detect illegitimate activity, contact us right away.

Safeguard Your PIN

ATM/Debit card PINs should be treated like passwords and kept secret.

- ✓ Ensure that you assign a strong/secure PIN to your card, avoid using the last four of your tax ID number, or date of birth.
- ✓ Shield the keypad when entering your PIN at ATMs or checkout terminals.
- ✓ Never share or write down your PIN.
- ✓ Update passwords and PINs if you believe your information has been compromised.

Safeguard Your Card Information

- ✓ Never provide your card number, expiration date, or security code over the phone unless you have initiated the call and trust the business.
- ✓ Be cautious of unsolicited emails, texts, or calls requesting account information.

Use ATMs Wisely

- ✓ Choose well-lit, reputable ATM, such as those attached to bank buildings.
- ✓ Avoid using machines that look damaged, loose, or altered.
- ✓ If something feels off, cancel the transaction and use a different ATM.

Skimmers:

A card skimmer is an illegal, hidden electronic device installed on ATMs, gas pumps, or payment terminals to steal card data. Skimmers were created to read magnetic stripe information, allowing bad actors to create counterfeit cards or process fraudulent transactions.

Common Types of Card Skimmers

ATM Overlay Skimmers ✓ A false card slot placed over the real card slot ✓ Often matching the machine's color and shape ✓ Often include an undetectable camera to capture PINs	**PIN Pad Overlays** ✓ A thin fake keypad placed on top of the real PIN pad ✓ Captures keystrokes as a person enters their PIN ✓ Usually slightly raised or "spongy" to the touch
Gas Pump Skimmers ✓ Installed inside the pump, out of sight ✓ Often Bluetooth-enabled allowing data to be retrieved wirelessly	**Deep Insert Skimmers** ✓ Inserted deep inside the card reader slot ✓ Invisible from the outside, making them often harder to detect by a card holder
Point-of-Sale (POS) Terminal Skimmers ✓ Terminals fraudulently replaced at retail stores ✓ Often capture both card data and PIN entries ✓ Most often used during busy hours or at busy locations to avoid detection	**Bluetooth or Wireless Skimmers** ✓ Hidden inside ATMs or pumps ✓ Digitally transmit stolen data to a nearby device

Below is an image of different types of skimmers.

Protect Your Card From A Skimmer:

Inspect the Card Reader

- ✓ Look for parts of the machine that appear loose, misaligned, or a different color.
- ✓ If the card slot wiggles or feels bulky, don't use it.
- ✓ When a card reader looks unusual, if possible, compare it to another nearby machine.

Inspect the Keypad

- ✓ A keypad overlay may feel raised, soft, or thicker than normal.
- ✓ If the buttons feel "off," cancel the transaction.

Tampering at Gas Pumps

- ✓ Choose a gas pump closest to the store entrance, these machines are often harder for bad actors to access.
- ✓ Look for broken security seals or loose panels

If Something Feels Off, Don't Use the Machine

Trust your instincts. If a machine looks damaged, unusual, or "off," choose another location.

For More Information On How To Detect A Skimmer:

Visit: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/skimming

To Report A Skimmer:

Visit the FBI's Internet Crime Complaint Center: www.ic3.gov