Be Aware! Credit Card Skimming Devices

We have received information about credit card skimming activity in the Cincinnati area. Skimmers are technical devices attached to automated teller machines (ATM) or point of sale (POS) machines, commonly at gas station pumps, that steal both electronic data and personal identification numbers (PIN) from credit and debit cards. There are several versions of ‘Skimmers’ some of which have become more technologically advanced; allowing data to be collected in bulk, from a distance, and without need for the skimmer device to be retrieved. Older versions of ‘Skimmers’ used radio frequency identification (RFID) to collect or transmit card data and a hidden camera to collect PINs. These older ‘Skimmers’ require portions of the device to be retrieved to fully collect card information; newer ‘Skimmers’ use micro-processing, Wi-Fi, and Bluetooth enabled technology to collect remotely without the perpetrator ever having to return.

Tips to Avoid Being “Skimmed:”

- Use ATMs from your banking institution, preferably ATMs that are in secured access areas and that are secured by cameras or monitors.
- For ATMs, inspect the device. Look for uneven colors or loose PIN pads and tug on the card slot before inserting your card.
- Check the machine for tampering. The presence of scratches, tape, or adhesive residue could indicate a fraudulent device.
- Avoid gas pumps where the tamper-safe security seal affixed to the pump has been broken or security tape that seems fake or out of place.
- Look at other nearby gas pumps or ATM card readers to see if they match the one you are using.
- Look above and around the keypad for suspicious cameras/miniature cameras.
- Place your hand over the keypad when entering your PIN.
- Always monitor financial statements for fraudulent activity.