PENNSYLVANIA STATE POLICE
COMMUNITY AWARENESS BULLETIN
CAB 002-22 September 12, 2022

SKIMMERS AND SHIMMERS USED TO STEAL PAYMENT CARD INFORMATION THROUGHOUT PENNSYLVANIA

The Pennsylvania State Police (PSP) is reminding Pennsylvania residents to be vigilant when using payment cards at ATMs, gas pumps, and other point-of-sale (POS) terminals at businesses. The PSP is aware of the use of skimmers at ATMs and POS terminals throughout Pennsylvania.

Skimmers are devices that fraudsters install at payment terminals to steal digital information found in the magnetic strip on the back of credit or debit cards. The fraudster can then copy the information to a blank card for use anywhere credit or debit cards are accepted. In addition to skimmers, shimmers are devices that fit inside the machine and copy information from the chip on the victim's card.

SHIMMER

Many skimmers are designed to fit over the original card slot and PIN pad. Some fraudsters utilize 3D printers to make parts to conceal the skimmer, which may make the ATM or POS terminal look different than a standard payment terminal. For example, a 3D-printed slot cover may conceal a light typically used to indicate where to insert the card.

ATM SKIMMER

Due to the increasingly sophisticated way skimmer/shimmer(s) are disguised, a victim may not realize their card information has been compromised until they recognize unusual activity on their account or receive a fraud notice from the card's issuer.

RECOMMENDATIONS

- Use secure payment methods, such as tap-to-pay or Apple Pay, Samsung Pay, or Android Pay whenever possible. These technologies are secure and very difficult for criminals to intercept. Use your card's magnetic strip only as a last resort.
- Use gas pumps or ATMs within sight of the building. Many fraudsters place skimmers away from busy areas in locations where they are less likely to be observed.
- Pay attention to the appearance of the gas pump or ATM. Some signs of tampering are:
  - Components that look or feel different from most of the machine
  - Tamper-resistant seal is broken on the gas pump
  - Graphics that are not aligned correctly
  - Machines that are side-by-side that look different
  - Buttons that do not work correctly or are hard to press

  If any of these seem to be the case, do not use that machine.
- Look for a potential skimmer with your cell phone. Go to Settings, then open the Bluetooth. If you see an unfamiliar device with a long string of random characters attempting to connect to your phone, that could be a skimmer.
- Review credit card and bank statements regularly to identify unusual or fraudulent activity.

PSP reminds residents who fall victim to a scam to report it to their local police department and to their financial institutions.