

ATM CARD SKIMMERS

Possible ATM Skimmer – on Thursday 04/10/25 a resident made a deposit at the **Wells Fargo ATM on Del Webb Blvd.** (She covered the keypad with her hand while entering code). On Friday 04/11/25, the Sacramento Wells Fargo Bank on Watt Ave notified her that someone had tried to use her ATM card but had declined it because they did not have the PIN code. This resident is in possession of her card, so she assumed that somehow her card was "skimmed" during her deposit at the SCLH Wells Fargo ATM on Del Webb Blvd. (This has not been confirmed as of this report).

What is Card Skimming? It is an illegal device that criminals attach to card readers at (ATM), Point-of-Sale (POS) terminals, or at gas pumps. Criminals can use the data captured from the magnetic strip to steal the victim's identity or create fake debit, credit, or Electronic Benefits Transfer (EBT) cards that can be used to make purchases and steal the victim's money or benefits. Card skimmers can be hard to detect because they are designed to blend into the terminal.

Recognizing Card Skimming Devices, Pinhole Cameras, and Fake Keypads:

- Most skimming devices fit over the original card reader; however, at gas stations, they can also be hidden internally behind the card reader.
- Fake keypad covers can also be used to record a PIN.
- Pinhole cameras can be placed above or around the PIN Pad or installed on the ATM to record a customer as they enter their PIN.

How to Avoid Card Skimming:

- <u>Visually and physically inspect</u> ATMs and POS machines before swiping or inserting your card. Does it wiggle or seem loose? If so, do not swipe or insert your card, notify the business and local law enforcement.
- Cover the keypad when you enter your PIN and never share your PIN with anyone.
- Use a chip-enabled card if you have one.
- <u>Use contactless-enabled cards</u> or phones for safe and easy payments by tapping your card or phone on a contactless-enabled payment terminal.
- <u>Sign up for notifications or alerts</u> for your bank and credit card transactions, and you will receive a notification or alert whenever your card is used.
- Pay with cash whenever possible. If you're ever concerned that your credit or debit card has been compromised, contact your bank immediately and request a new card.

PHONE SCAMS

A resident received a call claiming he/she had made various purchases on their Walmart credit card and was directed to call a certain number to verify the charges, Thankfully, this resident did not have a Walmart card and did not call back! Never give out any personal information to anyone you do not know. Never call back in response to an unsolicited phone call or email. When in doubt just hang-up the phone or delete the email. When in doubt contact a relative, friend or neighbor for advice.

We've received various reports with the following scenario: Caller claims you're a 2nd place winner of a jackpot (amount varies) and states the money will be directly deposited into your checking or savings account. To proceed, they request your account number and routing numbers. These scammers are very persuasive and often possess personal details such as your name, address, and sometimes additional information. To stop such calls, only answer if you know the caller. Important callers will leave a message. If you do answer, never share personal details with unknown callers. This also applies to emails and texts.

For more information visit the Lincoln Police Department's Technology Crimes webpage

