ATM Skimming Device

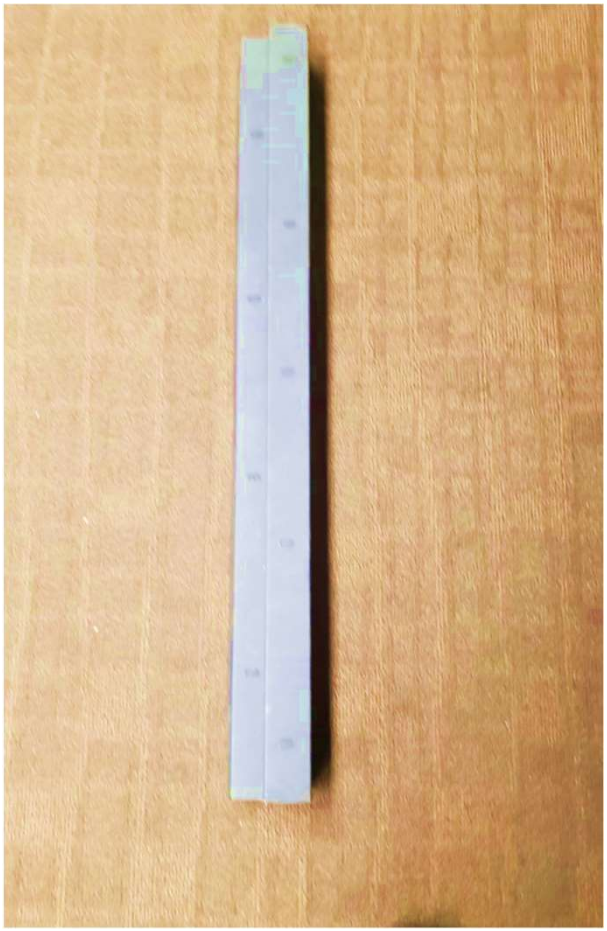
Los Angeles Police Department
Harbor Detectives

Detective Sergeant Raul Rodriguez 34014
2175 John S. Gibson Blvd.
San Pedro, CA 90731
310-726-7700

SKIMMING DEVICE

A skimmer is a card reader that can be disguised to look like part of an ATM. The skimmer attachment collects card numbers and PIN codes, which are then replicated into counterfeit cards. Skimming is the type of fraud that occurs when an ATM is compromised by a skimmer.

When you slide your card into an ATM that has a skimmer attached, you're unwittingly sliding it through the counterfeit reader, which scans and stores all your information from the magnetic strip as well as capturing your PIN from the keypad. This makes skimmers particularly dangerous compared to other forms of card compromise because the collected card data can be used to make ATM cash withdrawals.

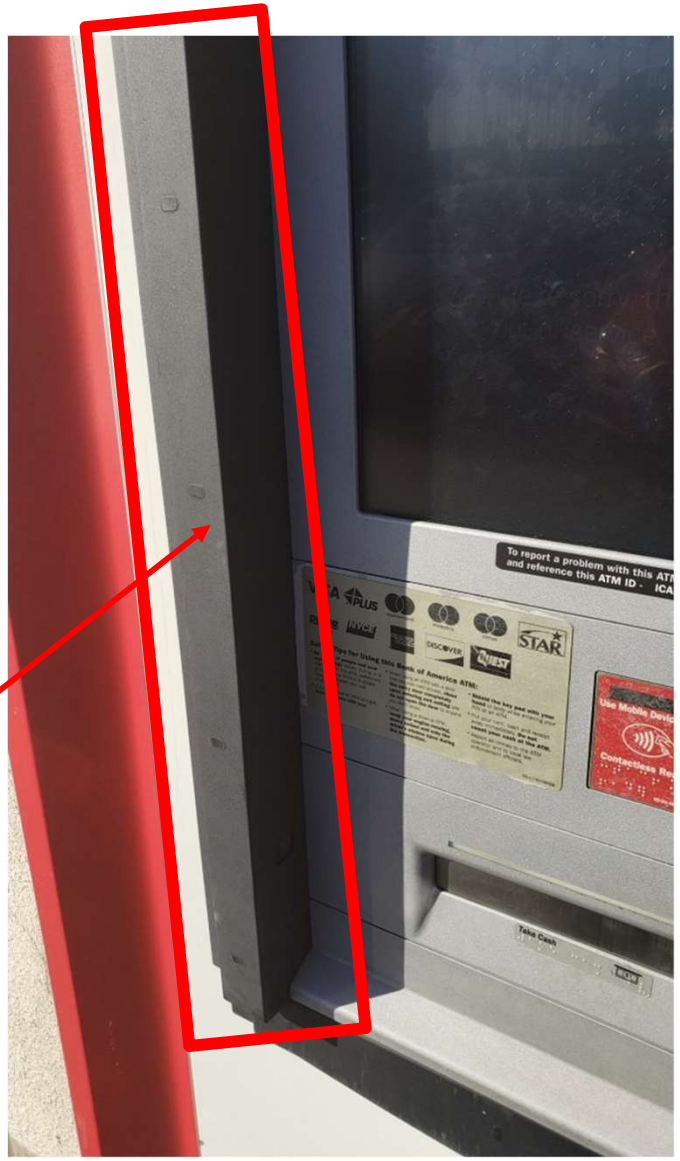


Actual skimming device found at a Bank Of America drive through in the Harbor Area.

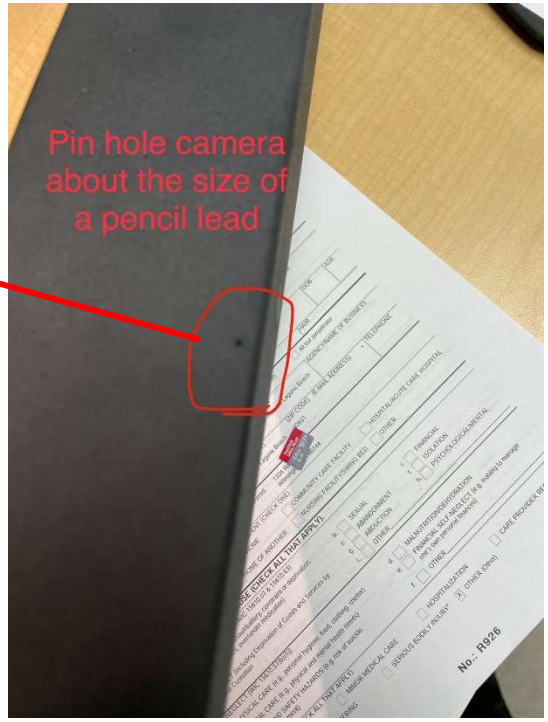
How to check for skimmers
The most frequently used methods of skimming are used on the card reader insert area. Before using an ATM, be observant of the following parts of the ATM:

PIN keypad
Card insert slot

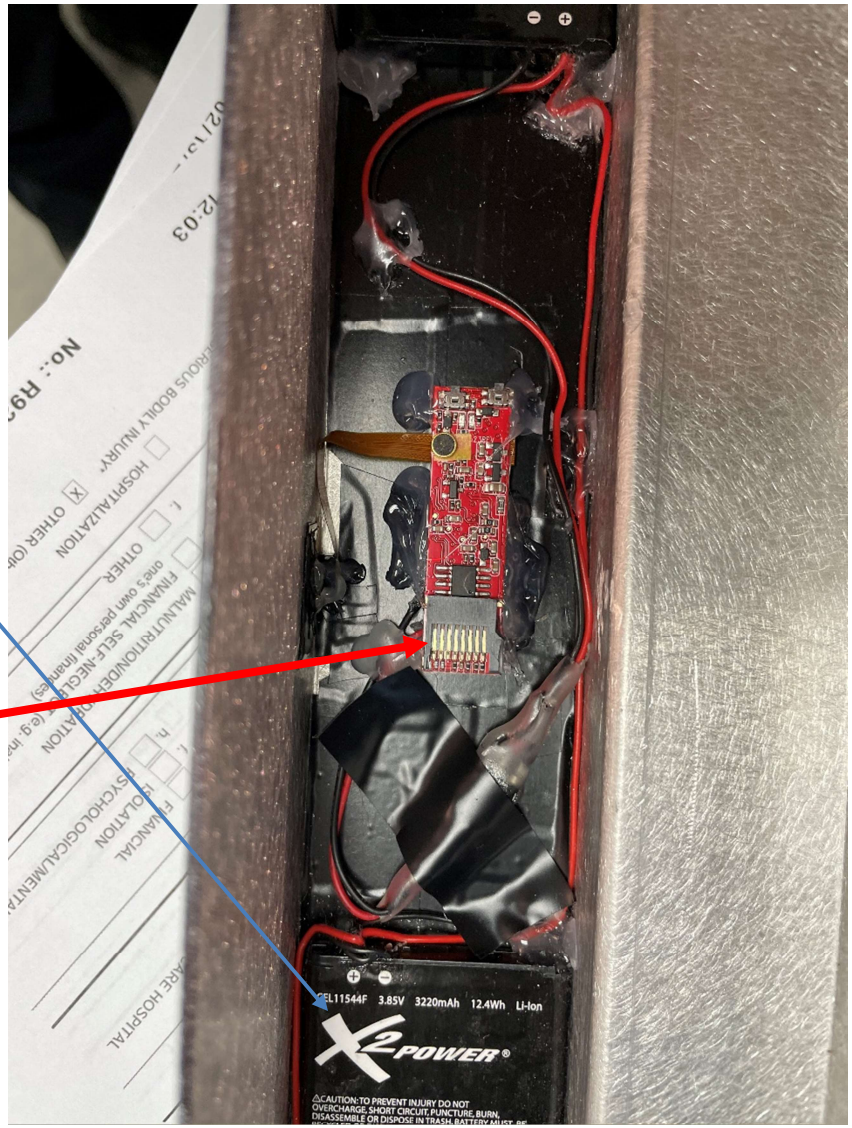
Skimming device placed on top of the ATM. Easily camouflaged into the ATM so that it will not cause suspicion.



The thief places a ‘pin hole,’ about the size of pencil lead, on the side of the device to capture the card holder’s key strokes from an integrated video camera.



Underneath the metal façade is equipped with batteries that will provide power to the integrated IC chip that captures the numbers on the victim's debit card and a 64 gig memory card to capture the card holder's pin code.



When visiting an ATM, check these parts for:

- Tape and/or sticky glue residue on any part of the ATM
- Bulkiness on the card insert area or the PIN keypad
- Anything hanging from the ATM
- Wiggle the card slot or keypad for loose-fitting attachments