

Skimming is the act of capturing cardholder data contained on the stripe of a credit, debit, or ATM card. Individual scams vary and are not limited to any one type of business; however, restaurants and gas stations appear to be the most common locations. Here is one possible scenario.



Customer uses credit card to pay for dinner.



Restaurant employee swipes card through small, concealed hand-held device to copy and store the account data.



The stolen card information is later downloaded from the device into a computer.



The information is then encoded on a counterfeit card or re-encoded on a lost/stolen card.

## Palm-Size Skimming Devices (READ/STORE)



Most battery-operated skimming devices are no bigger than a pager, but they can read and store the magnetic stripe data from 200 to as many as 3200 accounts.



When a card is swiped through the reader, the device copies all of the data encoded on the card's magnetic stripe. Some skimming devices have buttons that indicate whether or not the data has been captured and when the device is full to capacity. The device may also have a "kill" switch, which will erase all skimmed data.

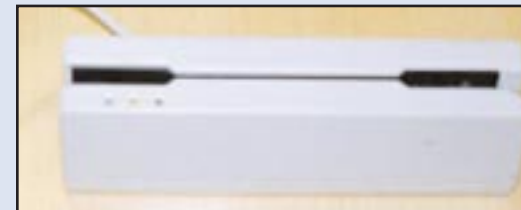


Full Indicator

Skimmer attached to Palm Pilot™ for data downloading.



## Portable Skimming Device (READ/WRITE/STORE)



A portable electronic skimmer, like the one shown here, can not only copy and store the data, but also can encode data from the magnetic stripe of a real or counterfeit card.

## TIPS

Should you come across a skimming device while collecting evidence:

- Do not tamper with any switches or buttons or try to open the device. You could delete the stored data and lose valuable evidence.
- Look for paraphernalia such as blank or printed cards, lists with account information, or other equipment associated with card counterfeiting. This can include diskettes, CDs, and electronic equipment such as printers, notebook computers, and cables. These items, when found together, can provide critical clues to the possibility and scope of the counterfeiting operations.
- Contact your local U.S. Secret Service office for assistance. Any attempt to extract data from a skimming device should be done by a technically knowledgeable person. U.S. Secret Service agents have the resources needed to download the data from the skimmers.
- Notify Visa Fraud Control (650) 432-2978 of any skimming incident and/or recovered devices.