

Credit Card Skimming Alert

FRAUD PREVENTION - Credit Card Skimming (courtesy of National Check Fraud Center, National Crime Alert Network, PO Box 80171, Charleston, SC 29416)

Credit Card Skimming



Skimming Device

A lot of press has been given to credit card skimming lately as it becomes more and more prevalent. You hand your credit card to the waiter or waitress at your favorite restaurant and you expect to pay for your meal, but sometimes that's not all you're paying for.

Credit card skimming is where account information is taken from the credit card (via the magnetic strip) and fed into a capture device (skimmer). Legitimately, this technology is used at merchant point of sale (POS) locations to gather the necessary credit information and charge the cardholders account. Criminally, this same information can be gathered and the perpetrator now has all the necessary account information needed to commit fraud on the account. Credit card skimming is thought to be one of the fastest growing forms of credit fraud today.

How The Fraud Occurs:

When a point of sale transaction is being processed at a merchant, the account information is transmitted for authorization. During this process, the information is captured in a storage device (skimmer). The account information can be compromised at multiple points during this process: The merchant location, within the transmission process or at the point of storage. Criminals typically connect a skimming device between the phone line and the credit card machine. When the account information is transmitted for approval, the criminal's skimmer device captures the account information that can then be utilized for fraudulent activity. Skimmers are as small as a typical pager and can easily be concealed and carried. This makes it extremely easy for a thief to capture your account information. The typical example of this would be in a restaurant. You give your waiter/waitress the credit card and they go in an off-stage area to process the sale. A dishonest employee could then take your card and swipe it through their own personal skimmer and capture your account information. The typical storage space on a skimmer would hold

approximately 100 account numbers. Most skimmers of this type are equipped with an 'erase button' which can delete all stored information with a single touch. This allows the criminal to quickly and easily destroy any evidence linking them to the crime.



Skimming Device

Frequently, individuals doing the skimming are employees of the establishment - often gas stations or restaurants. They will pull the small skimming device out of their pocket, swipe your card and hide it before anyone realizes what has happened. If they don't use the information themselves they are often paid a flat fee, or on a per card basis, for the information they steal. The skimmer captures your information and re-encodes it on the magnetic stripe of a plain plastic card or stores the information in the device itself so it can be downloaded later for illegal purposes. Yes, with one swipe of your card a criminal can take the information he or she has captured and make unauthorized purchases.



Skimming Devices

Consumer Tips:

- Try to keep an eye on your credit card at all times, if possible.
- Retrieve your credit card immediately after every transaction
- Keep your receipts.
- Review your account statements carefully, and notify your bank immediately of any discrepancies.
- Be on the lookout for portable skimming devices