



OSCEOLA COUNTY SHERIFF'S OFFICE
ROBERT E. HANSELL, SHERIFF



On the Dark Side of Credit Card Fraud

As you read this, a thief somewhere in the world could be using a counterfeit credit card with your name and account number on it.

Here's how its done...

Someone, somewhere made an extra swipe of your credit card. It could be a waiter or a store clerk or anyone you've handed your credit card to for payment.



Instead of just charging your card, the thief made an extra swipe of your credit card into a small hand-held device known a **skimmer**. Think of a skimmer as a net. It takes information right off the card itself.

The skimmer pulls the data from your card, giving the thief all the information needed to make a counterfeit card. A skimmer can hold card data from hundreds of different credit cards. Once this information has been downloaded into a skimmer it can be downloaded into a computer and e-mailed anywhere in the world. Credit card skimming has become a worldwide problem. Card losses due to skimming exceed \$1 billion a year. Skimming and counterfeit credit card scams are widespread in Europe, Asia and Latin America. They are a growing problem in the United States.

A Far East factory will do as many as 5,000 cards a night, and the next day those cards are in a suitcase on the way to Europe. Smaller scale skimming operations are common as well. Consider the scam ring in Florida, in which seven (7) people were indicted in April. Two waitresses skimmed a large number of credit cards from an Orlando restaurant. The waitresses then sold the credit card data to a middleman who sold the information to a group making counterfeit credit cards in Miami.

Skimmer Technology Improves

Ten years ago, skimming was much less common, Skimmers were too bulky to carry around and had to be hidden under counters. Smaller skimmers, roughly the size of a pager, hit the scene two or three years ago. These skimmers are easy to carry, easy to hide and easy to buy.



A few years ago you had to make a skimmer yourself. Now you can go on the Internet and buy one. Everything needed to pull off this crime is available on the Internet. A skimmer costs about \$300, and the equipment to make a counterfeit credit card cost about \$5,000 to \$10,000.

If it weren't bad enough, there's another kind of skimming going on as well. A thief slips a small, skimming bug into an older credit card terminal. The bug pulls credit card data from their terminal. A few days later the thief removes the bug. The bad guy comes and takes out the bugs and no one's the wiser.

What's happening to fight skimming?

For one thing, newer credit card terminals can't be bugged. And portable terminals, which would enable a waiter to swipe a credit card at a customer's table, are available, although not widespread. The U.S. Secret Service is working with the credit card industry to track down skimming rings by assembling a database of locations where scams have occurred.

As with any kind of credit card fraud, a consumer victim is not on the hook for the bill. Someone living in San Diego won't have to pay for a thief's \$5,000 shopping spree in Hong Kong with a counterfeit credit card.

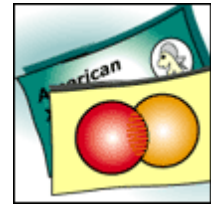
Know your rights

The Truth in Lending Act limits consumer liability to \$50 if a credit card is lost or stolen. And most issuers waive the \$50 fee. The hardest part for a fraud victim is straightening out their credit card report after a thief piles up charges in their name. It can take months to sort out. And that's why it's so important to monitor credit card bills carefully and report any suspicious activity immediately.

Look at credit card bill line by line.

Guard your credit card number; shred old receipts and bills.

Keep a close eye on your credit card when paying in a store, restaurant or gas station.



What to do if you become a victim

Clear your good name as quickly as possible.

Contact the three (3) major credit bureaus and have them place a fraud alert on your credit report.

[Equifax 800-525-6285](tel:800-525-6285)

[Experian 888-397-3742](tel:888-397-3742)

[Trans Union 800-680-7289](tel:800-680-7289)

Contact creditors for any accounts that have been tampered with or opened without your knowledge. Be sure to put complaints in writing.

Contact the [FTC \(877\) 438-4338](tel:877-438-4338). While federal investigators only tend to pursue larger, more sophisticated fraud cases, they do monitor identity theft crimes of all levels with the hope of discovering patterns and breaking up larger rings. Fill out the [ID Theft Affidavit](#) at the FTC's Web site, make copies and send to creditors. The agency also has an online complaint form.

Alert law enforcement, fill out a police report, and sign a written affidavit verifying that unauthorized transactions on your account are fraudulent. Send copies to creditors and credit bureaus as proof of the crime.