



ISSUE #14 – Fall 2005

- New Tricky Scam
- More Than Just Credit Card Fraud

New Tricky Scam -

While email and phone scams are rampant, a new scam shows how sophisticated and tricky identity thieves can be. This scam involves your existing credit card.

One day, you receive a call from a “Visa” or “Mastercard” representative saying, “This is (name), and I’m calling from the security and fraud department of Visa. My badge number is 92805. Your payment card has been flagged for an unusual purchase pattern and I’m calling to verify. This is on your Visa card, which was issued by (name of Bank). Did you purchase an Anti-telemarketing device for \$497.99 from a firm based in Arizona?” When you say “no”, the caller continues ...

"Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from \$297 to \$497, just under the \$500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?" You say "yes". The caller continues - "I will be starting a Fraud investigation. If you have any questions, you should call the 1-800 number listed on the back of your card (1-800-VISA) and ask for Security. You will need to refer to the following Control Number". The caller then gives you the 6-digit control number and asks "Do you need me to read it again?"

The **IMPORTANT** part...

The caller then says, "I need to verify you are in possession of your card". He'll ask you to "turn your card over and look for some numbers". There are 7 numbers; the first 4 are part of your main card number, the next 3 are the security Numbers' that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card. The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, "That is correct, I just needed to verify that the card has not been lost or stolen, and you still have your card. Do you have any other questions?" After you say No, the caller then thanks you and states, "Don't hesitate to call back if you do", and hangs up.

This scam is unique because you say very little and they never ask for or tell you the Card number. Why? Because they already have it! By getting the 3 security digits, they can now masquerade as you and make purchases over the phone or Internet by satisfying merchants who usually require “proof” of card possession by requesting the 3 security digits.

Neither your bank, credit union, Visa, nor any organization that you do business with should contact you and request any account or personal information. In the event you receive a call or an email, don't provide information, rather, check your records for the true phone number and investigate the nature of the call.

Have you checked your Free credit reports?

Under the FACT Act, you can review your credit report for free by calling 1-877-322-8228 or visiting www.annualcreditreport.com.

Be sure to review your credit reports for 1) accuracy and 2) possible fraud.

Have you placed a Free fraud alert on your credit file?

A fraud alert can restrict thieves from opening new accounts in your name. Call Equifax at: 1-800-525-6285, option 3.

Have you experienced identity theft?

Remember to contact Identity Fraud, Inc. for Free VRS Elite™ Unlimited fraud resolution services. Call:

1-866-4ID-FRAUD
(1-866-443-3728)



More Than Just Credit Card Fraud

If there are laws in place that leave me with little to no liability when it comes to credit card fraud, why is it so important to have added protection such as victim assistance and identity insurance?

Identity theft is more than just credit card fraud. There are over 25 different types of identity theft, credit card fraud happens to be the most common.

It's true that if someone gets a hold of your credit card number and charges a few hundred or thousand dollars on it, you will likely have little problem getting this resolved with your credit card company, bank, or credit union. The Fair Credit Billing Act establishes procedures for resolving fraudulent charges on your credit card accounts and the Truth in Lending Act limits your liability to \$50, a fee most companies waive.

ATM/ Debit cards... are not as secure. This money is cash coming straight from your checking or savings account, and you may be held liable for a much larger portion of the fraudulent charges. For example: if you report your card lost/ stolen or fraudulent charges after just two business days you could be liable for as much as \$500 of what a thief has taken.

Check fraud... Checks pose similar risk as ATM/ Debit cards. You lose the money right away and may not recover all of it in the end. So monitor your accounts.

Criminal identity fraud... What happens if you get pulled over for speeding and you quickly find yourself being questioned about a warrant that you do not have? Someone could have used your name and false identification for a prior criminal offense that was never taken care of, because they just walked away to let you take the fall. You may need to file an impersonation report at the original citing agency. In the more complex situations this could happen again and again due to lack of communication or documentation between agencies. What you think may be cleared up may still be on your record. You may even need to hire an attorney to clear your record and good name.

There is a long list of ways someone can gain by stealing your identity including: employment fraud, social security fraud, medical insurance fraud, and tax fraud. Identity Fraud, Inc can help you resolve nearly any type of identity theft and will even help reimburse you for certain expenses incurred in clearing your name.



Your best defense against fraud!