

December 12, 2008

Fraud Alert

With the holiday season fast approaching, thieves have come up with another creative way to steal your credit card information. The scam works like this:

The person calling says, "This is (name), and I'm calling from the Security and Fraud Department at VISA (or MasterCard.) My badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for \$497.99 from a marketing company based in Arizona?"

When you say no, the caller continues with, "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" because the address given is right.)

The caller continues with "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 (e.g. 1-800-VISA) and ask for Security. You will need to refer to this Control Number." The caller then gives you a six-digit number. "Do you need me to read it again?"

Here's the IMPORTANT part on how the scam works:

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 seven numbers; the first four are part of your card number, the last three are the security numbers that verify you are in possession 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 last three numbers to him. After you tell the caller the three numbers, he'll say, "That is correct. I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?" After you say no, the caller thanks you and states, "Don't hesitate to call back if you do", and hangs up. You actually say very little, and they never ask for, or tell you the card number.

What the scammers want is the three-digit number on the back of the card. Don't give it to them. Instead, tell them you'll call VISA or Master Card directly for verification of the conversation. The real VISA or MasterCard companies will never ask for anything on the card as they already know the information since they issued the card.

This alert was issued by the County of Wellington.

Contact: Mark Cloes,
Media & Community Services Officer,
Pager 1-888-806-3594.