NEW YORK STATE SENATOR

Simcha Felder

Warning: New Credit Card Scam

SIMCHA FELDER April 16, 2015

ISSUE: CRIME

Credit card scammers are continuously coming up with new ways to steal your information.

This new scam is particularly devious because the scammers actually provide ***YOU*** with information about your credit card, leading you to believe that they are a legitimate caller.

I urge you to be cautious and to never give your financial information to unknown callers. If you are suspicious about the caller you should hang up the phone and call the number on the back of your credit card.

The scam works like this:

The person calling says - 'This is (name) and I'm calling from the Security and Fraud Department at VISA. 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 card 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'.

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 this Control Number.” The caller then gives you a 6 digit number, and says, “Do you need me to read it again?”

IMPORTANT: The caller then says, “I need to verify you are in possession of your card.” He will ask you to “turn your card over and look for some numbers.” There are 7 numbers; the first 4 are part of your card number, the last 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 last 3 numbers to him. After you tell the caller the 3 numbers, the caller will 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 then 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 Scammer wants is the 3-digit PIN number on the back of the card**. ***Do not give it to them***. ***Instead, tell them you will call VISA or Master Card directly for verification of their conversation.***