KASRA Members:

This fraud has been around for a number of years, and is still being used. Please be on the lookout for this scam.

VISA & MasterCard Telephone Credit Card Scam

This scam is pretty slick since they provide YOU with all the information, **except the one piece of information that they want.**

Note, the callers do not ask for your card number; they already have it. This information is worth reading. By understanding how the VISA & MasterCard Telephone Credit Card Scam works, you'll be better prepared to protect yourself.

An employee was called from "VISA", and another was called the next day from "Master 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?" **Note that there is no need to send it to you since the credit card company need only reverse the charge on your account.**

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. "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 7 numbers; the first 4 are part of your 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 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. But after the call on Wednesday, the employee called back within 20 minutes to ask a question. He is glad he did! The REAL VISA Security Department told him it was a scam and in the last 15 minutes a new purchase of $497.99 was charged to the card.

Long story - short - the employee made a real fraud report and closed the VISA account. VISA is reissuing a new number. **What the scammers want is the 3-digit PIN 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 their conversation. The real VISA told the employee that they will never ask for anything on the card as they already know the information since they issued the card! If you give the scammers your 3 Digit PIN Number, you think you're receiving a credit. However, by the time you get your statement you'll see charges for purchases you didn't make, and by then it's almost too late and/or more difficult to actually file a fraud report.

What makes this more remarkable is that on Thursday, an employee got a call from a "Jason Richardson of Master Card" with a word-for-word repeat of the VISA scam. This time he didn't let him finish. He hung up and filed a police report, as instructed by VISA. The police said they are taking several of these reports daily! They also urged the employee to tell everybody he knows that this scam is happening.

Remember: Do not give anyone any information solicited over the telephone. If you have any doubts, call the telephone number on the back of your credit card.

Submitted by Evo Alexandre