

FRAUD ALERT

CREDIT CARD SCAM

Legitimate callers from your MasterCard or VISA companies do not have to ask you for any numbers. THEY ALREADY HAVE THEM!

This is the latest scam used to get your credit card information:

1. You may receive a call from the **Security and Fraud Division** at MasterCard or VISA.
2. They may sound legitimate to the extent that they give you an ID number (which is fake).
3. They will already have some of your account information such as your credit card number, your address, etc.

This is a typical scenario:

“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 or MasterCard) which was issued by (name of bank or credit union). Did you purchase an Anti-Telemarketing Device for \$497.99 from a marketing company 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 your address – they are just confirming their information), is that correct?”

When 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 and ask for the Security Department. You will need to refer to this Control Number (a random 6 digit number). Do you need for me to read it again?”

NOW, THIS IS THE KEY TO THE SCAM WORKING!

The caller then says, “I need to verify you are in possession of your card. Turn your card over and look for some numbers. There are 7 numbers and the first four are part of your card number. The next three are the security numbers that verify that you are the possessor of the card. (These are the numbers you sometimes use to make Internet purchases to prove you have the card in hand. The caller will ask you to read the last three numbers to them. After you give them the three security numbers, they will say, “that is correct. I just needed to verify that the card has not been lost or stolen and that you still have the card. Do you have any other questions?”

After you say no, the caller thanks you and hangs up.

WHAT THEY ARE LOOKING FOR ARE THE THREE DIGITS ON THE BACK OF YOUR CARD! ONCE YOU GIVE THEM YOUR 3 DIGIT PIN THEY WILL THEN BEGIN TO MAKE PURCHASES ONLINE USING YOUR CARD NUMBER AND VERIFYING WITH THE 3 DIGIT PIN YOU GAVE TO THEM.

GIVING THEM THE THREE DIGITS ALLOWS THEM TO MAKE PURCHASES AS IF THEY ARE THE LEGITIMATE CARD HOLDER.

DO NOT UNDER ANY CIRCUMSTANCES GIVE ANYONE YOUR THREE DIGIT PIN IF THEY CLAIM TO BE FROM YOUR CREDIT CARD COMPANY!

The company that issued your card ALREADY KNOWS THE THREE DIGIT PIN! THEY ISSUED IT IN THE FIRST PLACE!

IF YOU RECEIVE A CALL OF THIS NATURE, TELL THEM YOU WILL HAVE TO CALL THEM BACK THEN CALL THE 800 NUMBER ON THE BACK OF YOUR CARD AND ASK FOR THEIR SECURITY DEPARTMENT. EXPLAIN THE REASON FOR YOUR CALL. ONLY BY CALLING THE 800 NUMBER YOU HAVE CAN YOU BE ASSURED THAT YOU ARE TALKING TO YOUR CREDIT CARD COMPANY!

