CREDIT CARD SCAM EXAMPLE

1. You receive a call from someone posing as they are from "VISA", or "MasterCard". 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 bank. Did you purchase an Anti-Telemarketing Device for $497.99 from a marketing company based in Arizona?"

2. 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?"

3. 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 #" The caller then gives you a 6 digit number. Do you need me to read it again?"

4. Here's the IMPORTANT part on how the scam works. The caller then says, "he needs 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 your card number, the next 3 are the 'Security Numbers' that verify you are in possession of the card. These are the numbers you use to make Internet purchases to prove you have the card. Read me the 3 numbers". 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.

Mississippi Attorney General's Office Consumer Protection Division 2013