

## PHISING SCAM

**From:** GSA

**Sent:** Thursday, August 06, 2009 11:19 AM

**Subject:** New Phising Scam

**Importance:** High

Good morning AOPCs -

The Office of Charge Card Management wants to alert you to a new phising scam that has occurred with employees at the Social Security Administration (SSA). Please advise your cardholders of the following:

- Do not give out ANY personal information over the phone, the internet or the mail.
- If you think the request is valid you should always contact the bank yourself using the number on the back of your card.
- If anyone ever gives out information they should immediately call their bank.

**Note:** The callers do not ask for your card number; they already have it. By understanding how this works, you'll be better prepared to protect yourself. An SSA employee was called on Wednesday from 'VISA', and another call was received on Thursday from 'MasterCard'.

### **The scam works like this:**

**Caller:** 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 (MasterCard) 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',

**Caller:** 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'.

**Caller:** 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 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.**

**Caller:** 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... please read the 3 numbers to me.

After you tell the caller the 3 numbers.

**Caller:** 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.

**Caller:** Thank you and don't hesitate to call back if you do.

You actually say very little, and they never ask for or tell you the Card number. But after SSA was called on Wednesday, the SSA cardholder called back within 20 minutes to ask a question. The REAL VISA Security Department told us it was a scam and in the last 15 minutes a new purchase of \$497.99 was charged to the card.

SSA made a real fraud report and closed the VISA account. VISA is reissuing them 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 your card issuing bank directly for verification of their conversation.. The real VISA told them 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.

Please pass this on to your cardholders, family and friends. By informing each other, we protect each other.

Kind Regards,  
U.S. General Services Administration

Office of Charge Card Management