

TYPES OF SCAMS & CONS

Internet Buyer Con:

This con scheme starts with a legitimate and honest person selling something on the Internet. A buyer agrees to a price, but needs to ship the item out of the country. The buyer overpays for the item and asks the seller to send the overpayment to the shipping company. The result is that the naive customer deposits a worthless check he received from the alleged buyer and then sends off the extra cash by Cashier's Check or wire. When the check is later returned, the customer sustains the loss.

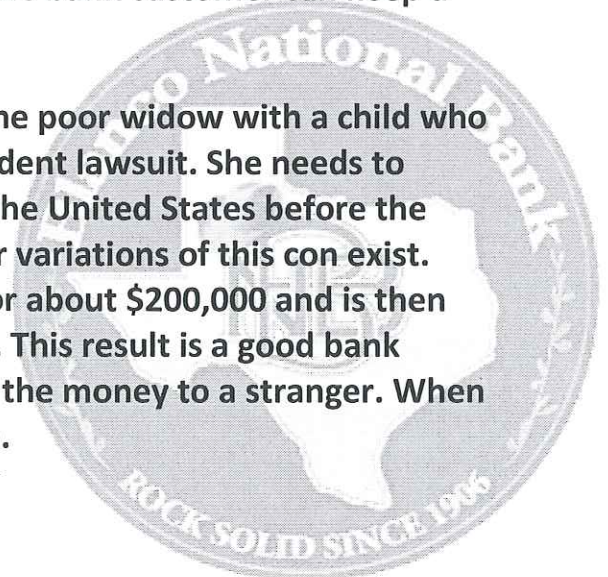
In some variations of this con scheme, a very large check is received made payable to the seller. The con claims it was an error but says he would greatly appreciate it if the seller could just send him back the extra \$87,000 (or some other amount) overpayment, and keep \$500 for the trouble.

In other variations, the seller is told he will receive a wire, but in reality the bank receives a Fed-Ex package containing a large check and instructions to deposit it to the good customer payee's account. The customer thinks he has received good funds by wire and doesn't even realize he has cashed a bogus check and sent the money to a stranger.

The Help Move Money Con:

This started as the typical Nigerian Scam in which suckers are asked to help move millions into the country that has been funneled by foreign government officials. In exchange for the use of his account, the bank customer can keep a couple million dollars.

The more successful variation of this scheme is the poor widow with a child who just was awarded millions in an oil company accident lawsuit. She needs to move her money from Nigeria to a safe place in the United States before the corrupt government steals it. Hundreds of similar variations of this con exist. Eventually the bank customer receives a check for about \$200,000 and is then told to send 80 percent of the funds to someone. This result is a good bank customer cashing a worthless check and sending the money to a stranger. When the check is later returned, the customer is liable.



Lottery Scam Con:

In the lottery scam the customer is told he won a \$5,000,000 lottery, but the customer must pay the taxes and fees first. When the customer doesn't have the \$250,000 for the taxes and fees, the con has someone who can loan it to the customer. Your customer then deposits the check and sends the \$250,000 by wire. Again, the result is that the good bank customer cashes a worthless check for a stranger.

Debit Card 'Skimming' Scam:

This is a technique where people can create counterfeit ATM or debit cards by stealing your PIN and other account data and simply pull cash from your bank account. They set up equipment that captures the magnetic strip and keypad information when you input your PIN at ATM machines, gas pumps, restaurants, or retailers.

Don't type in your PIN at the pump - If you must use a debit card at the pump, choose the screen prompt that identifies it as a credit card so that you do not have to type in your PIN.

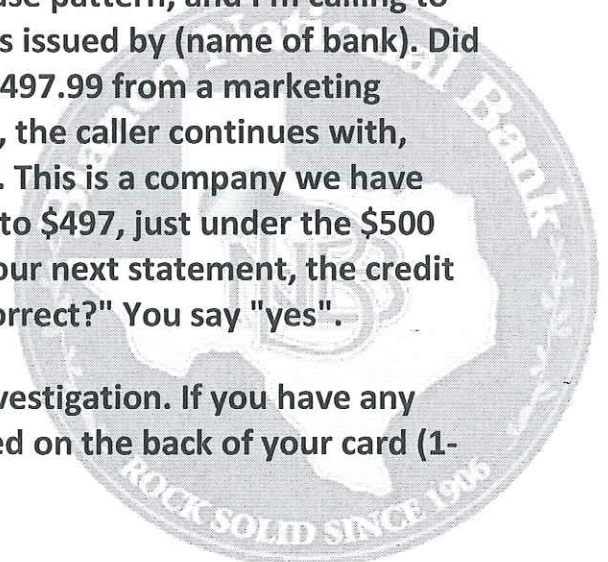
To reduce your risk at ATMs, use machines at banks rather than in convenience stores, airports, or any isolated locations.

Closely monitor your bank accounts - Check your accounts regularly. Don't wait for your monthly statement in the mail - sign up to view them online.

Visa & MasterCard Scam:

The scam works like this: 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 six digit number. "Do you need me to read it again?"

Here is the IMPORTANT part on how the scam works: The caller then says, "I need to verify that 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 last 3 are the Security Numbers that you 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, he'll say "That is correct; I just need 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. In reality the caller is using your Security Number and making a purchase with your card within 15 minutes of the phone conversation for the amount of \$497.99 (originally mentioned). Do not give out your Security Number to anyone! If you receive a call like this, tell the caller that YOU will call Visa or MasterCard directly to verify this.

