A New Credit Card scam!

Most of us now realize that we should NEVER, EVER give out our PIN = Personal Identification Number. 'They' usually ask for your "personal" PIN - Not the one on the card!

An example:

The person calling says, "This is {name} and I'm calling from the Security and Fraud department at VISA – (whichever) (name) - My Badge number is ######. Your card has been flagged due to an unusual purchase pattern, and I'm calling to verify the purchase". "This would be on your (name) card issued by {name} bank. Did you purchase a "whatever" for $497.99 from a marketing company based in Arizona? – (wherever)"?

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". Caller continues..."I will be starting a Fraud investigation. If you have any questions, you should call the 800 number listed on your card (1-800-(name)) and ask for Security. You will need to refer to this Control # ($$$ . . .".)

Then the person gives you a 6-digit number. "Do you need me to read it again?"
Caller then "needs to verify" that you are in possession of your card.

You are asked to "turn the card over"; there are 7 numbers on the back of the card; the first 4 are the last four digits of 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 last 3 numbers". You do so - then the caller says, "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? . . . 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.
What the scammer wants is the 3-digit PIN number. By the time you get your statement, you think the credit is coming, and then it's harder to actually file a fraud report.
The real VISA reinforced that they will never ask for anything on the card; they already know.

Jury Duty Scam

Here's a new twist scammers are using to commit identity theft: the jury duty scam. Here's how it works:

The scammer calls claiming to work for the local court and claims you've failed to report for jury duty. He tells you that a warrant has been issued for your arrest. The victim will often rightly claim they never received the jury duty notification. The scammer then asks the victim for confidential information for "verification" purposes.

Specifically, the scammer asks for the victim's Social Security number, birth date, and sometimes even for credit card numbers and other private information — exactly what the scammer needs to commit identity theft.

It's easy to see why this works. The victim is clearly caught off guard, and is understandably upset at the prospect of a warrant being issued for his or her arrest. So, the victim is much less likely to be vigilant about protecting their confidential information.

In reality, court workers will never call you to ask for social security numbers and other private information. In fact, most courts follow up via snail mail and rarely, if ever, call prospective jurors. Never give out your Social Security number, credit card numbers or other personal confidential information when you receive a telephone call.

This jury duty scam is the latest in a series of identity theft scams where scammers use the phone to try to get people to reveal their Social Security number, credit card numbers or other personal confidential information.

It doesn't matter *why* they are calling — all the reasons are just different variants of the same scam. Protecting yourself is simple: Never give this info out when you receive a phone call.

Delivery Charges

Recently a woman received a phone call late morning from Express Couriers to ask if she was going to be home as he had a delivery for her. He said he would there in roughly an hour. He turned up with a beautiful basket of flowers and wine. She expressed her surprise as I wasn't expecting anything like this and said she was intrigued to know who was sending her such a lovely gift. He said he was only delivering the gift and the card was being sent separately (the card has never arrived). There was a consignment note with the gift. The driver explained that because the gift contained alcohol he has to charge the recipient $3.50 as proof that he has actually delivered to an adult, and not left it on a door step if the recipient is out, to be stolen or taken by children. This seemed logical and she offered to get the cash. He then said that the company required the payment to be by Eftpos so he's not handling cash and everything is properly accounted for.

Frank was there and got his credit card and 'John' swiped the card on this small mobile machine that also had a small screen upon which Frank entered in his pin number. A receipt was printed out and provided. Later $4,000 was withdrawn from their credit account at ATM machines in the north shore area. It appears a dummy credit card was made using the details in the machine and of course, they had Frank's pin number.

Fraudulent Telemarketers

Who among us has not had the 'pleasure' of having a telemarketer, call us during our dinner hour – or if you work at home – any time during the day – saying something like 'Hello Mr. /Mrs. /Ms. Smith, how are you today'? (Like they really care?) Guess what? You are about to be subjected to a sales pitch for something. It could be for anything – literally anything, from stocks, to a telephone provider, to soap! The best thing to do, albeit impolite, is to hang up the phone! IMMEDIATELY ! SERIOUSLY ! Unfortunately, even though surveys today indicate that people are becoming more and more rude, uncaring, inhospitable, we, with few exceptions, will permit the caller to continue with his/her spiel, even if – in more and more instances - they trip over their tongues, cannot speak rudimentary, basic English. If you do not put the phone down, you are going to be subjected to a non-stop sales pitch for whatever product the person is hired to peddle.

The American Association for Retired Persons (AARP) has assembled an advisory list of Do's and Don'ts relative to telemarketing FRAUD. I hasten to add that not all of the telemarketers that you encounter are fraudulent, but some of them may be, and ALL OF THEM ARE ANNOYING. .

The Do's and Don'ts of handling telemarketers: (Best advice = HANG UP!)

- DO ask telemarketers for their company's name.
- Do call the Better Business Bureau.
- Do ask about the company's refund policy
- Do ask the company to send you written materials about products.
- Do talk to family, friends, lawyers, accountants before spending or committing money.
- Consider asking that your telephone number be removed from telemarketing lists.
- Do report suspicious telemarketing calls to the National Fraud Information Center (NFIC) at 1 800 876 7060.
- Don't pay for any prize.
- Don't allow any caller to intimidate or bully you.
- Don't give any caller your bank account number.
- NEVER, EVER GIVE YOUR PIN # TO ANYONE!
- Don't give your credit card number to anyone over the phone, unless YOU MADE THE CALL!

Ensure the Credit Card is Yours

A man at a local restaurant paid for his meal with his credit card. The bill for the meal came, he signed it, and the waitress folded the receipt and passed the credit card along. Usually, he would just take it and place it in his wallet or pocket. Funny enough, though, he actually took a look at the card and, lo and behold, it was the expired card of another person. He called the waitress and she looked perplexed. She took it back, apologized, and hurried back to the counter under the watchful eye of the man. All the waitress did while walking to the counter was wave the wrong expired card to the counter cashier, and the counter cashier immediately looked down and took out the real card. No exchange of words --- nothing! She took it and came back to the man with an apology.

Verdict: Make sure the credit cards in your wallet are yours.
Check the name on the card every time you sign for something and/or the card is taken away for even a short period of time. Many people just take back the credit card without even looking at it, 'assuming' that it has to be theirs.

FOR YOUR OWN SAKE, DEVELOP THE HABIT OF CHECKING YOUR CREDIT CARD EACH TIME IT IS RETURNED TO YOU AFTER A TRANSACTION!
REMEMBER – IT'S YOUR MONEY