

March 2006

This month we thought we would use our column to make folks aware of a scam that is making the rounds. Initially, we thought that maybe this would only be of interest and applicable to parents but after we thought about it, we realized that our children seem to use their (your) phones and the Internet more than their parents do! This scam has been attempted (sometimes successfully) both via telephone and e-mail.

The scam works like this: a person will call (but sometimes e-mail) their intended victim and introduce themselves as being from the "Security Department" of either VISA or MasterCard. The caller will tell you that your card has been "flagged" for an unusual "purchase pattern" and they are calling to verify that you made the purchase. The caller will tell you that the purchase was made on your VISA (or MasterCard) issued by (whatever your bank's name is). Seems legitimate so far, huh? Very considerate of them, right? Read on! The caller will ask you if you recently purchased an Anti-telemarketing Device (or some such fictitious but plausible-sounding gadget) for \$497.99 from "Company X" out of Arizona. Of course you didn't, you tell the caller.

The caller follows by telling you that VISA (or MasterCard) will be issuing a credit to your account and the credit will be sent to your current address, and they tell you your address and ask you if it is correct, and of course, you verify your address to them. The caller may also add that VISA (or MasterCard) has been "watching" this company for several months because this company has been fraudulently charging credit cards with purchases "just under the \$500 purchase pattern that flags most cards." The caller will then tell you that he or she will be starting a fraud investigation and if you have any further questions, you should call the 1-800 number on the back of your card, ask for "Security," and give the agent a 6-digit "control number," which of course the caller will cheerily provide you with.

Now, here is the most potentially detrimental part of the scam. The caller will tell you that they need to verify that you are actually in possession of your card. The caller will tell you to look on the back of your credit card and look for 7 numbers. The first four are the last four digits of your card's account number. What the caller will ask you to read to him or her are the last three digits, which are the randomly generated security numbers (a PIN number of sorts) intended to prove that you are in possession of the card and not just reciting the account number from memory or a discarded statement. Once you give the caller those three numbers, they will thank you and hang up. *Notice they never ask you for your 16-digit account number.* That's because they already have it—either from a discarded statement (or stolen from your mailbox) or maybe from an electronic intercept via the Internet. What they need to actually purchase something using your card without actually possessing it is those three numbers on the BACK of your card. The caller then hangs up and you or your child has just been scammed!

Seriously now, ask yourself: when have you ever heard of an enormous company like Elan (VISA) or MasterCard contacting every customer that makes a purchase of less than \$500? Or since when does a credit card company send a credit via mail to your residence—they would just credit your account, right? And furthermore, another red-flag should come up when the person tells you that they are just now starting a "fraud complaint." We thought they had already been monitoring Company X due to fraudulent practices—how else did they know to watch Company X in the first place? Besides, a customer always contacts a credit card company to make the fraud complaint, not the other way around, right?

Now, we don't mean to belittle the victims of this or similar scams. When we present it in a light-hearted way, it indeed sounds silly, doesn't it? In fact, many people fall prey to scammers every year from precisely just such a scam as I outlined above. They fall for it for basically two reasons: **#1**-they give you just enough industry-jargon, quickly and confidently, to make it sound legitimate enough, and **#2**-they catch you (or your children) off-guard and fluster you into giving them PIN numbers and account numbers when normally you would never fall for such a line of guff when you have adequate time to think these things through.

What you need to tell your children about these kinds of calls (or e-mails) is to never discuss identifying (especially financial) information with anyone over the phone and to refer the caller to you. Banks and credit card companies will never ask you to verify account numbers or PINs over the phone. They will only do this by mail or direct you to report this information in person to your local financial institution. Tell your kids to never give out the following information over the telephone or via email: **Dates of Birth, Social Security Numbers, Bank or Credit Card Account Numbers or PIN numbers.** Also, always make sure you are talking with a legitimate employee of whatever financial company they purport to represent. In this day and age, it is completely appropriate to ask the caller for his or her name, ID#, department and phone extension and then to call that person back using the number provided on your credit card billing statement or bank statement. Also, if you don't file your old statements, shred them; don't just throw them away!

While this example is only one of thousands of scams that are attempted upon unsuspecting citizens every year, we hope we've provided you with enough background on these scams to protect you and your loved ones from losing your hard-earned money and costing you possibly years of headaches trying to straighten out your credit history. Trust us, fighting "Identity Theft" can definitely be a real nightmare but you can easily protect yourself by using some common sense and doing some "verifying" of your own. Remember, an ounce of prevention is worth a pound of cure seven days a week and twice on Sundays!

Until next month, stay safe and say "Hi" to a cop once in a while!

The Fall River Police Department

*Don't forget to check out the Police Department web site, **www.fallriverpd.com***