ALEXANDRIA POLICE DEPARTMENT
CRIMINAL INVESTIGATIONS DIVISION
FINANCIAL CRIMES SECTION

COMMON SENSE INFORMATION AND TIPS ON HOW TO AVOID BECOMING A VICTIM OF "IDENTITY THEFT" AND HOW TO AVOID BEING "SCAMMED" IN SO MANY DIFFERENT WAYS.

Identity theft is the fastest growing crime in the United States today. Several different well-informed organizations have made information available on the subject by way of printed publications, Internet web sites and other sources of information. The intent of this document is to simplify what identity theft is, how to avoid becoming a victim, and how to recover if you become a victim.

One of the most important tools in recovering from an identity theft incident is an official police report. In years past, an identity theft victim usually would be told by whatever law enforcement agency they had contacted about the problem that they, the victim, would need to obtain a police report from the law enforcement agency where the criminal committed the crime. In short, if a thief opened a credit card account in another person's name, then used that card to make purchases in Baton Rouge, Lafayette, Lake Charles and Houston Texas, then the identity theft victim would have to go through the trouble of obtaining a police report concerning each of the unauthorized purchases from law enforcement agencies in each of the aforementioned cities. In some of those cases, the victim was told that they could not make a complaint over the telephone and it would have to be done in person, in that jurisdiction.

This situation quickly became a very troublesome problem for many victims. After hearing many such complaints from identity theft victims, the Louisiana legislature acted with an identity theft law that

provides the victim with an official police report from the law enforcement agency that has jurisdiction over the victim's physical address regardless of where the actual thefts or unauthorized purchases occurred.

That law, Louisiana Revised Statute, Title 14, chapter 67.16 reads in part: "Any law enforcement agency which is requested to conduct an investigation under the provisions of this subsection shall take a police report of the matter from the victim, provide the victim with a copy of such report and begin an investigation of the facts."

HOW DO I KEEP FROM BECOMING A VICTIM OF IDENTITY THEFT?

There is no ironclad guarantee that any person will **not** become a victim of identity theft in a normal lifetime. A person can however make it very difficult for a criminal to make them a victim. Follow some simple guidelines and you can protect yourself and your family from the fastest growing crime in the country today.

First off, what is identity theft and are there different types?

Identity theft is the intentional use or attempted use with fraudulent intent by any person of any **PERSONAL IDENTIFYING INFORMATION** (P.I.I.) of another person to obtain, whether contemporaneously or not, credit, money, goods, services, or anything else of value without the authorization or consent of the other person.

Types of IDENTITY THEFT:

>>>**Account Takeover** - your existing credit/debit card and account numbers are used to purchase products and services. (Most Common and often involves the **"precursor"** crime known as "unauthorized use of "access card" as theft" or "credit card fraud." {Both of those basically mean someone used your credit or debit card without your permission.} This crime becomes a true identity theft however when the thief causes any changes on the existing account by communicating with the card company or bank, claiming to be the **true card holder** and by doing anything like adding authorized buyers, changing the billing address or requesting additional cards.)

>>>**Application Fraud** - a criminal will use your P.I.I. to open new accounts in your name. (Common, but not as much as Account Takeover)

>>>**Criminal Identity Fraud** - your identity is taken to commit a crime, enter a country or commit acts of terrorism. (This is rare, but on the rise because of illegal immigration.)

What exactly is PERSONAL IDENTIFYING INFORMATION (P.I.I.)?

The most common bits are, but are not limited to your.....

SOCIAL SECURITY NUMBER
DRIVER'S LICENSE NUMBER
CHECKING ACCOUNT NUMBER
SAVINGS ACCOUNT NUMBER
CREDIT CARD NUMBER
DEBIT CARD NUMBER
ELECTRONIC IDENTIFICATION NUMBER
DIGITAL SIGNATURES
BIRTH CERTIFICATE
DATE OF BIRTH
MOTHER'S MAIDEN NAME
ARMED FORCES IDENTIFICATION NUMBER
EMAIL ADDRESS

How do identity thieves get your personal identifying information (P.I.I.)?

>They steal wallets and purses containing your identification as well as credit and bank cards.
>They steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.
>They complete a "change of address form" to divert your mail to another location.
>They rummage through your trash at home or the trash of your businesses for personal data in a practice known as "dumpster diving."
>They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for and a legal right to the information.
>They get your personal or business records at work.
>They find personal information in your home.
(Page 3)
>They use personal information you share on the Internet.
>They buy your personal information from "inside" sources. For example, an identity thief may pay an employee for information that appears on an application for goods, services or credit.

How do identity thieves use your personal identifying information?

>They call your credit card issuer and, pretending to be you, as to change the mailing address of your credit card account. The imposter then runs up charges on your account and because your bills are being sent to a new address, it may take some time before you realize there is a problem.

>They open a new credit card account using your name, date of birth and other bits of your P.I.I. When they use the card and don't pay the bills, the delinquent account is reported on your credit report.

>They establish telephone or wireless service in your name.

>They open a bank account in your name and write bad checks on that account.

>They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

>They counterfeit checks or debit cards, and drain your bank account.

>They buy cars by taking out auto loans in your name.

While the aforementioned things are more the rule than the exception, a growing percentage of identity thieves are now obtaining state issued driver's licenses with their photograph on it but with a victim's personal identifying information. What would happen if that thief got stopped for speeding and was issued a traffic ticket? Do you think he's going to pay the fine? And whose door are the police going to show up at with an arrest warrant after the due date on the ticket passes?

WHAT SHOULD I DO IF I BECOME A VICTIM OF IDENTITY THEFT?

Follow these three steps.
>1. Contact the fraud department of one of the three major credit reporting agencies and request that a **FRAUD ALERT** be placed on your credit history.

(Note: As of 02-19-2007 and according to the website requesting a fraud alert with any one of the three credit reporting agencies, will automatically notify them all.)

The three credit reporting agencies are:
(Equifax: 800 525 6285; P.O. Box 740241, Atlanta, GA. 30374-0241)
(Experian: 888 397 3742; P.O. Box9532, Allen, TX. 75013)
(TransUnion: 800 680 7289; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA. 92834-6790)

If you have not already done so, have your **credit file disclosure** run. (Commonly referred to as a credit history report or credit report.) You can obtain a free credit report every 12 months. To do so, go to this website on the Internet:

www.annualcreditreport.com (You will be asked several times if you care to purchase some type of "credit security" or "an alert service that will notify you of someone's inquiry into your history". These are offered by any of the three reporting agencies. You can purchase this service if you wish to but it is **not** required to obtain your free report.) If you do not have access to the Internet, call one of the toll free telephone numbers listed for Equifax, Experian or Trans Union and request your report be sent to you by the U.S. postal service.

>2. Contact the creditors or companies for any accounts that have been tampered with or opened fraudulently and inform them of the situation.

>3. File a police report with the local law enforcement agency that has jurisdiction over your physical address and/or the agency in the community where the identity theft(s) took place.

>>>It is strongly suggested that you contact the Federal Trade Commission (F.T.C.) and ask to be sent a booklet named "**I D THEFT, WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME"**
Or go to the F.T.C. website and download the same information found in the booklet. The information will be very helpful in stopping the damage being done to your credit history by an identity thief and will tell you how to begin the process of repairing it.

You can contact the F. T. C. by going on line at or call toll free at 1 877 IDTHEFT (1-877-438-4338).

After you have done all of the aforementioned and if the crime committed against you in any way involved the Internet, you can go to this website, www.ic3.gov . Here you will be able to report what has happened to you to the Federal Bureau of Investigation and an organization named the National White Collar Crime Center. The F.B.I. and NW3C, in partnership, formed this website as an identity theft intelligence clearing house to report cyber crime. They look for similarities in these types of crimes and forward important suspect information to the appropriate law enforcement agency for the area that those crimes have been committed in.

WHAT ARE SOME OF THE THINGS I CAN DO TO KEEP FROM BECOMING A VICTIM OF IDENTITY THEFT?

>Guard especially your social security number. It is the key to your credit report and banking accounts and is a prime target of criminals.

>Monitor your credit report, yearly. It contains your social security number, present and prior employers, a listing of all account numbers, including those that have been closed, and your overall credit score.

>Shred all old bank and credit card statements, as well as "junk mail" credit card offers, before trashing them. This includes checks from old checking accounts. Buy a good shredder for your home. Crosscut shredders are a little more expensive than a standard shredder but worth the extra cost.

>Do not carry extra credit cards or other important identity documents except when needed. Carry only one or two cards you use on a daily basis.

>Copy the contents of your wallet on a photocopy machine. Copy both sides of your driver's license and credit cards so you have all the numbers, expiration dates and telephone numbers if your wallet or purse is stolen.

>Do not mail bill payments and checks from home. They can be stolen from your mailbox. Mail them from a post office.

If you live in an area where reports of mail theft are common, you may want to obtain a post office box at a local post office or have some kind of secured mail drop box at your home. Check with the post office before installing any kind of locking mailbox. Some of them are **not** approved by the postal service.

If you or another member of your household stays at home all day, familiarize yourself with the usual time the mail is delivered and retrieve it as soon as it's dropped off.

>Do not have your social security number, date of birth or drivers license number printed on your checks.

>Order your Social Security Earnings and Benefits statement once a year to check for fraud.

>Examine the charges on your credit card statements before paying the bill.

>Cancel unused credit card accounts.

>Subscribe to a credit monitoring service that will notify you whenever someone applies for credit in your name. (The three major credit bureaus and most credit card companies provide this service for a monthly fee.)

Keep personal and vital information in a secure location.

How many people come into your home that you might not otherwise expect to? Examples: Friends of your kids, a utility service repairman, relatives. The list could be a long one. We all would like to think that any person who would be invited into our homes are going to be people of outstanding character. Most very likely are but there is no way for you to know that for sure. Why tempt fate? Keep your important paperwork and documents under lock and key or in a secret location away from curious eyes.

CAN IDENTITY THEFT HAVE AN EFFECT ON BUSINESSES?

Most of the time, when people hear the term "Business Identity Theft" they think of a situation where a person has represented himself as an employee of a business, that he does not work for, then does something like make unauthorized charges to that companies account or commit some other business oriented scheme for monetary gain. While situations like that certainly have occurred, the kind of **Business Identity Theft** that all

businesses or organizations should be mostly concerned with is the theft of personal identifying information on customers, clients and patients by an employee who has access to that information. This type of crime is especially troubling to any business or practice in the **medical field.** Doctors offices, physical therapy clinics, medical supply companies, home health services and a host of others not listed here, have the kind of vital, personal information an identity thief covets the most. Business identity theft is not something that most employers and/or managers really want to think about but should give a lot of consideration to.

"I had no idea that a trusted and dependable employee would ever have done anything like steal vital information on a customer or patient in order to make some kind of financial gain."

You might be very surprised to know how many times in one day that phrase is uttered to a law enforcement officer somewhere in the United States. Any business person who thinks that way, needs to get a grasp on the reality of the twenty-first century. **"Employee information theft"** is unfortunate but is a fact of life. Another fact of life is that an employer or manager can not know about all of the things that go on in an employee's life. As well as you may think you know someone, you might be shocked to find out certain things about a person. Now, this does not mean you can't trust your employees. Without a certain degree of trust in all employees, a company would eventually grind to a halt.

The two following "hypothetical stories" should sum it up.

"Fred owns and manages a company that has 21 employees. He has a long list of customers and has that customer information, including credit card and checking account numbers, in the data base of his company's computer. All of his employees have access to that information even though the only people who really need access

to it are the two ladies in the office who process the orders and bill the customers. The guys on the loading dock, the delivery drivers and the janitor don't need access to that information. But its only a click away for any of them to see on any of the companies computer terminals. One of Fred's delivery drivers, Gary, is going through a rough time at home. His wife recently lost her job, they have a special needs child whose medications cost them about $450.00 a month and they just moved into a new house in a neighborhood they always wanted to live in. Gary realizes he has to come up with a solution to an immediate financial crisis or he and his family are going to lose what they have worked so hard for. He thinks about the conversation he had with "Sam" who he ran into at the hardware store and who used to work for Fred's company but was fired over a year ago. Sam told Gary that he knew a guy who paid $50.00 a name for the personal and vital information on real people. The same kind of information that is stored in Fred's company computer that anybody who works there can access."

"Cindy works at a doctor's office. Her duties consist of scheduling appointments, checking patients in and out and fielding general telephone calls for the doctor or nurses. All of her work can be accomplished with the office computer and telephone. There is no patient information stored in the office computer. That is all stored in the file room in folders that have those color and number combinations on the folder tabs to identify a particular patient. These folders contain detailed information on patients such as dates of birth, social security numbers and the patient's mother's maiden name. The mother's maiden name is included in this particular case because of family medical history.
Cindy has a gambling problem. She lost a lot of money over the past weekend at a casino. Her rent and car payment are due this week and she still has to have money to eat and go out with her friends. Payday isn't for another ten days. Cindy thinks about the cousin of an acquaintance she met while she was out dancing at a club last week. He was an interesting guy who became really interested in her when he learned that she worked for a doctor and he had good money to pay for information that was in those files at the office. She didn't have to steal anything, he said. All she had to do was write down certain bits of information from the file and put it back in the file room which was directly behind her work area. Handling those files was not really part of her job. Only the doctor and nurses were supposed to see them. But she was often asked by some of them to look up or put back a file on busy days. That would give her the justification to be in the file room."

I didn't give any ending to either of these stories so you could draw your own conclusions. What will "Gary" and "Cindy" do? These two fictional characters very likely could be tailored to an employee in any workplace. If you own a business, ask yourself this question: **"Who are the people that work for me that need to have access to certain information in order to do their job?" If there is no reason for any other employee's to have access to certain information, then don't give them access to it.**

It's no reflection on that person's trust worthiness. They just simply need to know what the details of their job are and that their job does not require access to certain information. Also let the employees who have access to vital information know that there is an identity theft law that applies to any situation dealing with the unauthorized release of vital information and that it is something that they very likely would be arrested for should they break that law. **The bottom line is this. If your company or practice does not have policies or rules dealing with who has access to customer or patient information, it is not a matter of if information theft is going to happen but when is it going to happen.** If you have not already done so, establish strict rules concerning this situation and enforce them. If you don't, you are likely going to be sued by an angry customer or patient who became a victim of identity theft and can show liability on part of your business or practice.

THINGS YOU AND YOUR LOVED ONES SHOULD KNOW ABOUT OTHER TYPES OF FINANCIAL RELATED CRIMES, THE INTERNET AND THE TELEPHONE.

Be aware of **"PRETEXTING"**. Pretexting occurs when you receive a telephone call and the caller says that he/she is a representative of your credit card company. To convince you of this, they will tell you your credit card account number. It is not as hard as you may think for thieves to get your credit card account number. Remember, this is what they work at doing. But just being armed with the account number does not mean they will be able to run rampant with it. They will primarily attempt to use your number to make on-line purchases via the Internet. In recent years, the credit card companies became more aware of this problem so they added an additional security feature to your credit card. It is that small grouping of numbers usually found on the back of the card in the signature block and it usually will consist of anywhere from 3 to 7 numbers. This is true with all major credit cards like MasterCard, Visa and Discover. This however is not always the standard. American Express uses a group of numbers as a security feature but they will have some numbers on the front and back of the card.

Just be aware of this, because if you ever receive a call like this, the thief will be **"PHISHING"** for that small group of numbers. **They have to have those numbers to make an on-line purchase in most cases.**

Also be aware of **"PHARMING"**. Pharming occurs when a criminal creates an Internet web site that will look like the legitimate web site you might be searching for. The purpose of this is to try to get a user to log onto that bogus site, thinking they are on a legitimate site and then get the user to surrender vital information. If you have ever accessed one of the Internet search engine sites, such as **Google, Ask, Bing or A.O.L.find,** then you know that after you enter the "key words" for whatever you are looking for, you will be given anywhere from one to hundreds of millions of choices of web sites that are associated with the key words of whatever you are looking for. I will use **American Express Credit Card** company as an example. In March of 2006, I typed in the words "**american express**" into Google's search engine. I was given 347,000,000 (347 million) sites to choose from. How many of these that actually had something to do with the credit card company were legitimate and how many were counterfeit? I have seen counterfeit American Express web sites that rival the very authentic ones. **Just make sure that if you access a web site to do business on line, that you are at the right address.**

"PHISHING" also applies to other situations.
Never give any personal information over the telephone to anyone who has called you stating that they are an official representing a credit card company, bank, insurance company, government agency or any other organization. Identity thieves will pose as anyone and will tell you anything in order to obtain vital or personal information from you. One of the most popular lies they use would go something like this: "I am Mr. So and So with the ABC insurance company. There is a problem with your account. We have to verify some information otherwise your policy could be in jeopardy." or "I am Mr. So and So with the Social Security Administration. We have detected some fraud on your account and have to verify some information." They then will go on asking you to provide your social security number or perhaps bank account number. In these situations, **THERE IS NO WAY FOR YOU TO KNOW WHO YOU ARE TALKING TO**. These days we have the advantage of "caller ID" on most telephones in order to critique such calls. Still don't be fooled by one of these calls. Thieves will open a telephone account with some type of official sounding name attached to it so that name will show up on your caller ID. It doesn't matter how "official sounding" the person is, tell them that you do not give such information over the telephone. **Don't be intimidated by the caller. Even if they tell you something like they are a government official calling to find out "why didn't you show up for jury duty and you're in big trouble". They will say something like that at the first part of their call to throw a person "off balance" and make them more susceptible to release personal information. After all, who wants to be fined or jailed for missing jury duty? Now, you might get a call from a legitimate government agency one day for some reason. If you suspect deception or dishonesty on part of the caller, then follow the instructions listed later in this paragraph about calling the company or agency back after you have verified**

the correct telephone number and ask to speak to the person who called you. In any situation like this, a legitimate caller will understand your reason for doing so.

IT IS VERY IMPORTANT TO TEACH YOUR CHILDREN ABOUT THESE TYPES OF TELEPHONE CALLS. MOST CHILDREN WILL BE INTIMIDATED BY SOMEONE WHO SPEAKS WITH THE VOICE OF AUTHORITY AND THEY MAY REVEAL INFORMATION TO A CALLER. Do **not** even give information that you think could not be used against you. **Credit card companies and government agencies already have your personal or vital information. Remember, you gave it to them when you opened the account.**

If the caller persists, then tell him something like this. "Very well, please give me your name, your company or agency name and the physical address". (Not a post office box number.) Ask for a telephone number but do **not** call it to verify the authenticity of the call you have received. (There could be a person working in collaboration with the person who called you. That second person could be answering your call to the number given to you by the first caller. The second person could then give you false information telling you that the first person who called you was legitimate.) If the caller gives you the information you requested, then verify it by calling telephone information yourself and giving the organization name along with the city and state information provided by the caller. If information tells you that there is no such listing for that city and state, then very likely you had been speaking to an identity thief. If there is such a listing, then you could call them back if you choose to. Remember, the only time you should give your personal information to someone over the telephone is when you have initiated the call to a legitimate company or government agency.

A note on a "not too often thought about subject"……

Deceased family members.

There comes a time in our lives that we have to deal with the reality of family members dying. Most often it is going to be a case of adult children burying their parents. When this time comes, usually when the last parent or another relative dies, all or most of the surviving children or relatives will get together to take care of or close out the deceased persons personal business. Some examples of that would be closing out credit card and bank accounts and dealing with insurance companies. If and when you find yourself in this situation, remember this.

Many people have discovered that a thief has used their deceased parent or other relatives name to do something like purchase a vehicle or open several credit card accounts months after they have died. It is imperative that the deceased family member's mail is diverted to a safe delivery address. Identity thieves read newspaper obituaries to see which people have recently died and will go to the deceased person's home several days afterwards in the hope of stealing the mail. Treat a deceased family member's name and personal identifying information as though the person is still living.

COUNTERFEIT CHECKS & MONEY ORDERS

The Internet has opened up for thieves a "hunting ground" that covers the entire globe. Many of these thieves speak the English Language because they realize that English is the "language of money" and your money is exactly what they will be attempting to separate you from. Here are the two most likely scenarios involving a person receiving an **"Unexpected Large Sum"** check or Money Order in the mail.

1) **(In this first scenario, I'm going to use the name "Ted" as the thief.)** You "meet" Ted via the Internet**.** You develop a sort of relationship with Ted and spend lots of time "chatting". **(Ted looks for people who exhibit a vulnerable or naive demeanor in their conversations. He is looking for people who are "lonely" or may have just gone through a relationship "break up" of some sort. He can spot such a person quickly and he will use that vulnerability in his favor.)** Ted will eventually breach the subject with a vulnerable or naive person about getting help in getting a check cashed. The "vulnerable" person will usually jump at the chance to help in order to feel useful or needed by someone. The "naive" person will usually do it simply because they are not well enough informed or experienced with everyday life in the real world. It is very likely that Ted is going to show more interest in the "relationship" than the person who ends up being the victim. The way Ted pops the question can have many versions but it will sound something like this. "Can you help me with a check that I am trying to get cashed? I'm not an American citizen and don't have a bank account in your country. For doing this favor for me, I'm going to give you part of the money. When you receive the check, put it in your bank account, send my part back by electronic transfer or just mail one of your personal checks to me. You keep the rest." Then about a week or so later, the check Ted asked your help with and that you deposited into your bank account is returned to your bank marked as counterfeit. The personal check you sent to him has already been cashed and once money has been transferred electronically, you can't get it back.

2) You all of a sudden receive a letter in the mail telling you that you have won the **lottery** in a foreign country or that you have won a **sweepstakes or contest** or that you have been selected as a **"secret shopper"** who makes purchases at businesses in your area and reports on the service you received. You wonder about this because you've never bought a lottery ticket from a foreign country **(which by the way is illegal according to federal law. United States Criminal Code, Chapter 61, section 1301.)** or entered any sweepstakes or contest or applied to be a secret shopper. The letter goes on and answers the question you have just asked yourself. "Your name and address were entered as a result of a random drawing from the telephone directory in your area" or "Your name and address was selected from a national marketing list". You may now be thinking "Well, OK, that's how they got my name," so, you read on. The letter is accompanied by a check made payable to you or the check will arrive in a different

mailing a few days after you receive the first letter. But the letter states that before you can cash in you winnings, you have to pay a processing fee or some type of tax to that country's lottery system or whatever. The letter will also likely say something like "Because of the lottery or contest security protocol, you are being advised to keep your winning information confidential until your winnings are processed." Some of the more elaborate schemes may even include a working telephone number for you to call an "account manager" to help you "finalize the payment process and get your funds to you as soon as possible." This "account manager" is just going to be one of several thieves that make up part of the entire scheme. You call the number and are told how to proceed. You wire transfer or send off a check for the "taxes, processing fee" or whatever they call it. You soon discover that the check sent to you is worthless but your money is already gone.

Many people ask "How is it possible for someone to generate a counterfeit check which rivals or in some cases is even better looking or of better quality than an authentic check?" There is no regulation of blank check stock any where in the country that I'm aware of and there are check printing programs for personal computers on the market today by the dozens. That's how!

As with many great ideas or inventions throughout history, something intended to benefit society has been twisted by the criminal element. The blank checks and printing programs were intended essentially to help business owners save money by printing out their own payroll checks as opposed to paying someone to do the same thing. The thieves know this and have bought thousands of these blank checks and check printing programs. Then they put any information they want to onto the checks. **If for whatever reason you decide that there may be some legitimacy to the check you have received and deposit it into your bank account with the "wait and see" thought on your mind, be advised of one thing. Federal banking regulations require banks to give "credit" to a person's account after they have made a deposit into that account, within a certain number of days of the deposit. Be warned that the credit the bank gives for a deposit is usually called "conditional credit". What does that mean? In plain spoken American-English it means that until that check or other negotiable document has cleared absolutely the financial institution of it's origin and the actual funds have been received by the bank that accepted the deposit, that check remains questionable as to it's validity.**

CREDIT / DEBIT CARDS WITH COMPUTER CHIP TECHNOLOGY (SMART CARDS)

In the first part of the twenty first century, several companies began experimenting with "smart card" technology in earnest. This technology employed the use of a small computer chip that was embedded in the plastic card itself. That computer chip essentially replaced the magnetic stripe that is still seen on most cards today. The magnetic strip or the embedded chip carries the cards electronic information. These "smart cards" were thought to be a leap forward insofar as added security was concerned. They known in the industry as "CONTACTLESS SMART CARDS". And as the name implies, that's exactly how they are used. They make no contact with a card reading device. The devices that have been around for a while that we slide our cards through when making a purchase with a credit/debit card are known as P.O.S.T. (**P**oint **O**f **S**ale **T**erminal) units. The sliding action allows the device to make contact with the magnetic strip on the card and then reads its account information. The use of the card often times has to be accompanied by the entry of a P.I.N. number.

A "Smart Card" never has to touch the contactless card reading device. All a user has to do is wave the card over or near the device and the device captures it's information in a fraction of a second. This is how that happens. The contactless card reader emits a "magnetic field" that will "energize" the computer chip embedded in the card causing it to transmit its information.

This is where a potential problem comes in. The legitimate manufactures of these contactless card readers are not the only people who make them. A person in possession of electronic technology "know how" can build one as well. Unfortunately for the vast majority of us who play by the rules, these surreptitious or clandestine card reading devices can work just as well as the real thing at capturing your cards electronic information. That information can then be used to create a cloned credit/debit card.

HOW DOES A THIEF GET INFORMATION OFF OF MY SMART CARD AND WHAT CAN I DO TO STOP IT?

The clandestine card reading devices need a fair amount of computing power to work. Most will be attached to a laptop computer. All a thief has to do is get within about two (2) to three (3) feet from a smart card in order for the device to capture its information.

Think about this. How many times have you seen a person standing in the checkout line at a business carrying a laptop computer case, briefcase, large purse or any other such item that could carry a laptop computer? How many times has such a person stood

within about three (3) feet of you or where you credit/debit card was? It doesn't matter if your card is tucked away in you wallet under layers of other plastic cards, paper, leather or whatever. The clandestine card reader will very likely still be able to emit enough power to energize the computer chip and then capture its information.

This of course does not mean that every person that you see from now on standing in line somewhere with some type of carrying case is there to steal your smart card information. In the first place, you have to have a "smart card". All of these cards that I've seen so far have some type of identifying feature indicating that they use computer chip technology. If you have such a card or receive one in the future, there is a way to shield your card's information from "prying" eyes.

There is a company named "IDENTITY STRONGHOLD" that manufactures a secure credit card sleeve that prevents any magnetic transmission from reaching your card. As long as the card is in this sleeve, it is safe from the unauthorized capture of its information. There may be other such companies that manufacture these types of secure card sleeves, but this is the only one I'm aware of at this time. You can contact this company at its website, or call telephone # 800 610 2770.

Sources of information:
Federal Trade Commission
Better Business Bureau
The International Association of Financial Crimes Investigators (IAFCI)
The National White Collar Crime Center (NW3C)

IF YOU HAVE A QUESTION CONCERNING POSSIBLE IDENTITY THEFT, FRAUDULENT SCAMS OR ANY OTHER FINANCIAL RELATED CRIME, FEEL FREE TO CALL THE ALEXANDRIA POLICE DEPARTMENT'S CRIMINAL INVESTIGATIONS DIVISION AND ASK TO SPEAK TO A FINANCIAL CRIMES INVESTIGATOR. 318-441-6416 or 318-441-6460

SGT. Lee Leach
Updated: January 2010

Criminal Investigations Division
Financial Crimes Section / Supervisor