Being a Victim of Fraud

You should not feel foolish. Fraudsters make dozens of attempts for every one time they are successful. They exploit people who are trusting and sincere. They have had a lot of time to hone their craft. You now know that it is time to take an active part in protecting your PII, your identity and yourself.

CONTACT YOUR LOCAL POLICE

It is important for the police to be able to screen your problem. If there is a local connection, an investigation can be initiated. If it is something like a Nigerian Scam or Tax Fraud, they can direct you to the resources necessary to help you with your problem.

CHECK YOUR CREDIT HISTORY

If you were the victim of Identity Theft, your credit history may give insight into the person by whom you were defrauded. If the fraudster didn't steal your ID, he may have sold your PII to someone who is trying.

MAKE A REPORT TO A MAJOR CREDIT BUREAU

Trans Union, Equifax, and Experian are the three major credit bureaus in the United States. Every time you apply for credit, a record is made with each one. Your credit is examined by each one and they make recommendations on your credit and actually calculate Beacon Scores. They all have Fraud Alert plans. Contact them at their website.

THE CREDIT FREEZE

The credit freeze is not for everyone. The credit freeze will cause any attempts to obtain credit with your PII to be denied. It is free to freeze your credit, but it costs money to unfreeze it. It can be done through the three major bureaus as well. You can also partially freeze it or dictate to what extent you want your credit verified before it is granted.

OBTAIN LEGAL COUNCIL

In extreme cases of Identity Theft, an attorney may be needed to aid in the mending of one's credit. This is only in extreme cases, where tens of thousands of dollars of damage has been done. People who have found houses and cars purchased with their credit by scammers have been served well by obtaining council.

Conclusion

Fraud is not going away any time soon. The age of the Internet and electronic media everywhere you go is making it easier and easier to commit fraud. Be cognizant of what you do with your PII, use common sense when dealing with electronic media, and always be cautious to whom you give your PII and you can seriously decrease your chances of being defrauded. The best fraud prevention is education.

If you have been a victim of fraud, make a report to:

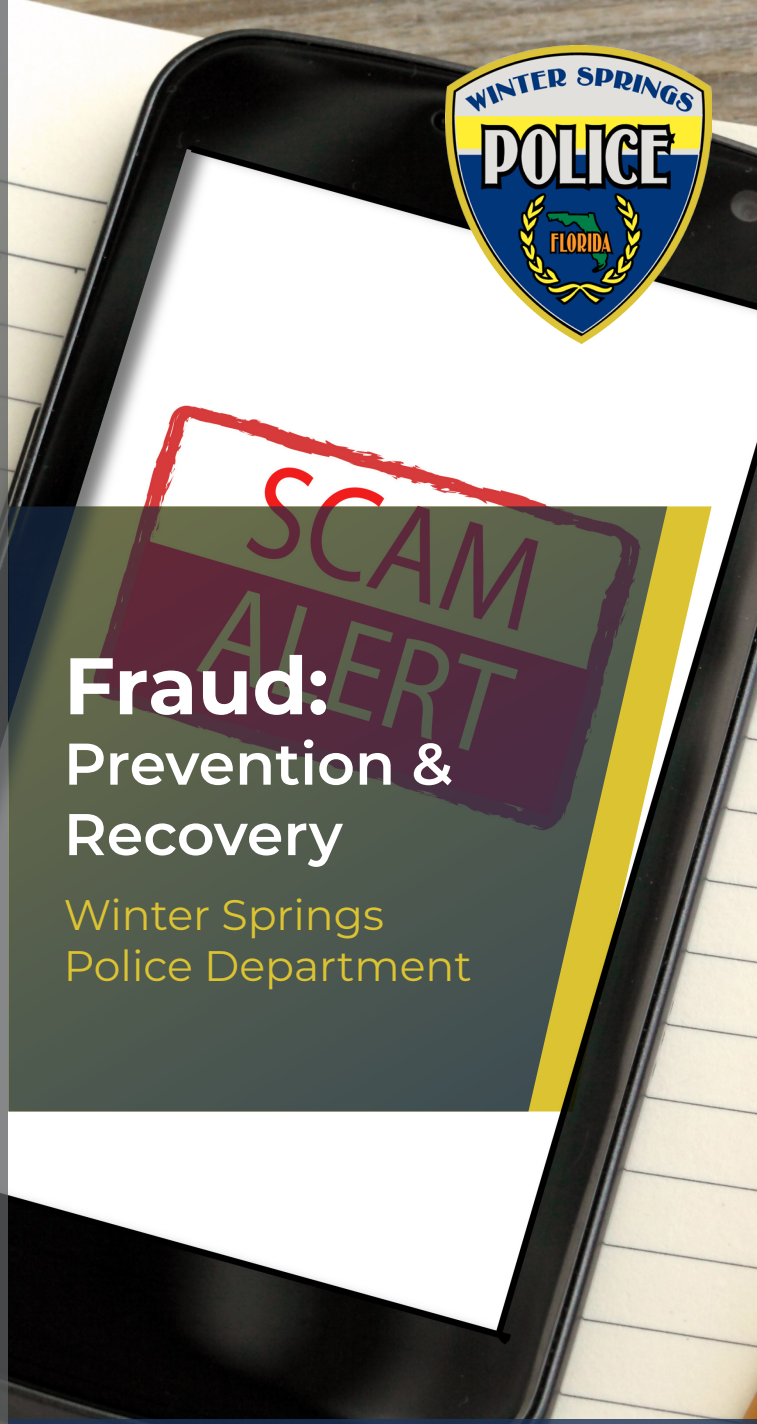
Credit Reporting Bureaus - www.transunion.com
www.experian.com
www.equifax.com

Internal Revenue Service - www.irs.gov

Federal Trade Commission - www.ftc.gov

Internet Crime Complaint Center - www.ic3.gov

Winter Springs Police Department
300 North Moss Road
Winter Springs, FL 32708
Emergency: 911
407-327-1000
www.winterspringsfl.org



Fraud:
Prevention & Recovery

Winter Springs
Police Department

Winter Springs Police Department
www.winterspringsfl.org

Identity Theft

Identity theft is the use of an individual's or entity's *PII* (personal identification information) to access someone's existing financial information or create credit. Identity Theft can often be perpetrated using the smallest amount of your information. Pre-approved credit applications that contain your name and address should be destroyed. Make sure you closely safeguard all of your PII. Don't open links in unsolicited emails. Avoid using paper checks with vendors with whom you are unfamiliar, and never give out personal information over the phone.

Advance Fee Scam

An Advance Fee Scam occurs when the victim pays money to someone in anticipation of receiving something of greater value—such as a loan, contract, investment, or gift—and then receives little or nothing in return.

The variety of advance fee scams is limitless. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or any other "opportunities."

If the offer of an "opportunity" appears too good to be true, it probably is. Know who you are dealing with. If you have not heard of the person or company, learn more about them. Understand fully any business agreement that you enter into. If the terms are complex, have them reviewed by a competent attorney. Be wary of businesses that operate out of PO boxes or mail drops and do not have a street address. Also, be suspicious when dealing with persons who do not have a direct telephone line and who are never in when you call, but always return your call later.

Secret Shopper

Scam artists seek to take advantage of people who may be looking for additional income. People believe they are hired as a "secret shopper," but instead are scammed out of their own cash. The Secret Shopper Scam operators convince consumers they will pay them for shopping by sending them a check that later turns out to be a fake. The fraudster will convince them to wire a certain amount of the fake check to them, while assuring them that they can keep the remainder of the money to purchase the agreed-upon goods or services as a "secret shopper." Once the scammer receives the wire transfer, they disappear, and the individual's money is lost for good. Don't become a victim of this scam!

Mail Scam

You may receive a flyer for credit consolidation, offers to refinance your home, insure your water line, extend your auto warranty, or have your air conditioner serviced. Often, these are phishing attempts. If scheduled, they may show up to your home and use that opportunity to gather PII about you. If you pay by check, they can obtain your checking account information. Anything to steal your identity and money. Make sure to use licensed and insured contractors for any home repairs.

Email Scam

Other scam artists operate by email, you may know it as Spam. Spam often contains live links to valid websites. By valid it is meant that they are functioning, legitimate websites. When you click on them, however, you get something other than what you expected. These can often contain phishing attempts or fake websites which look just like your banking website or a retail website which you normally trust. Spam can also contain an attachment. Do not open any unsolicited attachments. They can contain payloads which carry viruses. A virus can damage your computer but a virus can also capture information from your computer and send it back to the hacker. The hacker can design a virus to recognize numbers which match the pattern of credit card numbers and bank account numbers. The virus can collect everything you enter into your computer, every keystroke! That information can be used to compromise your identity. Be very careful with Spam.

Phone Scam

Phone scam? But I'm on the Do Not Call List! A merchant (or scammer) can use a computer- generated dialing system IF at some point you have been a customer or associate of theirs. A very liberal interpretation of this is being used to generate polls and surveys. Computer-generated calling will also ask "if you would like to be excluded, press #" or something like that. Hang up. Don't press anything. Your response involves you in what they are doing and they will continue to call, which of course leads to more phishing. Unfortunately, political polls and non- profit groups are not included in the Federal law. The Grandma Scam is the scam where a phone call is made with the premise that the caller is a law enforcement official calling on the behalf of someone who has been victimized or incarcerated. They will then attempt to convince you that they need bail money or airline ticket money and that it needs to be wired. The easiest way to debunk this is to have them give you the name of their agency, not the number, and contact them yourself. If you call the number they give you, the only person you will get on the phone is the scammer. If it is truly an emergency, they won't ask for any money.

Tax Fraud

Tax season brings about many shocking revelations. Nothing is more shocking than finding out a tax return has already been filed with your name and Social Security Number, but the refund isn't coming to you! The Internal Revenue Service investigates all matters of Tax Fraud. The IRS does not share information with local law enforcement. By contacting the IRS on their web page, you can file a complaint regarding a fraudulent return. It is very simple to commit this type of fraud and nearly untraceable. The Federal Government is just beginning to scratch the surface in this area, and hopefully in the future we can see this type of fraud disappear.

When most of us think of fraud, we think of something that is phony or fake, but fraud is something very real and it affects all of us as Americans. Fraud is defined by Webster's as: intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right.

Fraud affects all Americans by raising banking costs, insurance rates and the prices of retail goods and services. Victim businesses inadvertently must pass on the cost of being victimized by fraud and the cost of fraud prevention. Fraud is costing the United States billions of dollars every year. Fraud comes to us in a countless number of forms and a huge variety of configurations. The bottom line, however, is always the same. Fraud is an attempt to deceive a person in order to separate them from their liquid assets.