IDENTITY THEFT

PROTECT YOUR MONEY

WHAT IS IDENTITY THEFT

Identity Theft is a common term used for all types of crimes in which someone wrongly obtains and uses another personal data in some manner that involves fraud or deception, usually for economic gain. Identity theft is the fastest growing white-collar crime in the nation. Identity Theft cost Americans $16 billion in 2014. Every 2 seconds someone is a victim of Identity Theft.

HOW IDENTITY THEFT IS COMMITTED

- **Shoulder Surfing – Someone watching you punch in your credit card or pin number at an ATM.**
- **Business Records Theft – Someone steals personal information from a business or institution where you are a customer, patient or employee.**
- **Scamming – Someone sends an e-mail, posing as a legitimate company with the purpose of obtaining personal information.**
- **Phone Fraud – Establishing cellular phone service in someone else's name.**
- **Skimming – When someone uses a special date collection device known as a "Skimmer" to steal credit and debit card numbers as the card is being scanned/processed to pay for merchandise.**
- **Dumpster Diving – When someone goes through your trash to obtain copies of checks, credit cards, bank statements or other records.**
- **Mail Theft – Someone stealing mail to get new credit cards, bank or credit card statements, tax information as well as falsifying change of address information.**
- **Theft of A Wallet or Purse – The thief obtains personal information from the theft of your purse or wallet.**
- **Social Media – Someone obtains information that you have shared over the Internet.**
- **Spoofing and Phishing – When thieves set up look-alike websites of legitimate businesses and trick consumers into entering their personal information by sending e-mail messages that warn them that their account is about to expire or has been accessed illegally.**

WARNING SIGNS OF IDENTITY THEFT

- **Your monthly credit card and bank statements suddenly stop arriving.**
- **You are denied credit for reasons that you do not understand of your financial position.**
- **You start getting bills from companies you do not recognize.**
- **You receive calls from collection agencies or creditors for an account you don't have or that is up to date.**
- **You observe unusual entries on your credit report.**
- **Financial account statements show withdrawals you didn't make.**
- **A creditor calls to say you've been approved or denied credit that you haven't applied for; or, you get credit card statements for accounts you don't have.**

What is a "Skimmer"

A skimmer is a small hand held device that captures card holder data contained on the stripe of a credit or debit card. Skimmers can hold information from hundreds of cards. The information is downloaded from the skimmer to a computer and then can be sent anywhere in the world. Your credit card can be skimmed at a restaurant, gas station, hotel or any place you hand over your credit card. All an employee has to do is to make an extra swipe of your credit card through a small, concealed hand held device.

10 ways to protect your credit cards

1. **Never leave your credit card unattended at work.**
2. **Don't leave your cards in your car.**
3. **Do not write down your personal identification number (PIN). Memorize it.**
4. **Always make sure your card is returned to you after purchase.**
5. **Always keep your cards in a secure location especially when traveling.**
6. **Report lost or stolen cards immediately.**
7. **Sign the back of new credit cards as soon as you get it with a permanent marker and destroy unwanted cards so no one else can use them.**
8. **Make a list of your credit cards and their numbers. This information is vital for reporting lost or stolen cards.**
9. **Always check your monthly statement. Make sure the charges are yours and report any discrepancies.**
10. **Only give your credit card information over the phone if you have placed the call to make a purchase from a reputable company.**

SCAM ALERT - 8 SCAMS TO LOOK OUT FOR

1. **IRS Scam – When victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the person refuses to cooperate, they are then threatened with arrest.**
2. **Fake Prize, Sweepstakes, Lottery Scam – You receive an e-mail claiming that you won a prize, lottery or gift, and you only have to pay a 'small fee" to claim it. The person is told that he/she must send money to pay for administration fees and taxes. The prize, of course, does not exist. No genuine lottery asks for money to pay fees or notifies it's winners via e-mail.**
3. **Romance Dating Scam – A person out of nowhere finds you on a single's site and starts professing their love for you in a short time. The individual then tells you he/she is currently working or living in a foreign country, and experiencing trouble cashing their paychecks. The con artist nurtures an online relationship and convinces the victim to send money or cash the checks sent in the mail. "That's right" the checks are counterfeit.**
4. **"419" Nigerian Scam – You receive an e-mail, fax, or letter usually written in capital letters. The individuals are representing themselves as foreign government officials or persons in need of assistance, offering the recipient the "opportunity" to share in a percentage of millions of dollars. They will ask you to place large sums of money in overseas bank accounts. Next, they explain to the victim in great detail that the money is for taxes and legal fees. In reality, there is no money, except for the money that comes from your account.**
5. **Green Dot MoneyPak Cards – An individual representing a company or business informs a caller of an unpaid balance on a bill. The individual convinces the caller of the company's validity by confirming the person's name, date of birth, and social security number. If the caller is eager to pay the bill, he or she is then instructed to go to CVS Pharmacy and purchase a Green Dot MoneyPak Card. After placing the money on the card the con artist will instruct the caller to give them the pin number that is printed on the back of the Green Dot MoneyPak Card. Once given the pin number, the con artist will immediately withdraw the caller's money.**

Green Dot MoneyPak Cards are reloadable debit cards not linked to a banking account.

6. **Grandchild Scam – A Grandparent will receive a call from someone claiming to be their grandchild. The caller says he/she is in jail located in a foreign country. The caller needs money for bail and then informs the caller on instructions where to send the money via Western Union.**
7. **Past Due Utility Bills – Businesses are most likely to receive these types of calls. The con artist informs the business they are in arrears, and unless payment is made immediately, utilities will be disconnected within the hour. The con artist then demands payment through means of a prepaid card or wire transfer.**
8. **Check Cashing Scams – Victims are approached by strangers or acquaintances, and asked to cash a check for them since they do not have a bank account. Many times, the scammer will offer the victim a small amount for their troubles. The checks are often deposited at a nearby ATM, then cash is immediately withdrawn. When the check returns as fraudulent, the victim is out any cash that was withdrawn from their account.**

What Is Front Porch Theft

Front Porch theft is when thieves target parcel and packages left on a front porch. Thieves are even known to follow UPS trucks and patiently wait and watch as package(s) are placed on the front porch or door steps. Even those who track the shipping information online do not know exactly when the driver will be delivering the packages. Unfortunately, there will always be a window of opportunity for thieves to steal packages.

Protect Your Good Name

There are some simple steps people can take to minimize the risk of becoming a victim of Identity Theft.

- **Guard your social security number. Give it out only when it is absolutely necessary.**
- **Minimize the amount of personal financial information and credit cards you carry. Memorize passwords and PINS instead of carrying them with you.**
- **Keep personal information in a secure place in your home. Shred identifying information before throwing it away.**
- **Do not give sensitive information to unsolicited callers. Remember that the most legitimate businesses will not ask for your Social Security or bank account numbers.**
- **Shield your hand when entering your PIN at a bank ATM or when making long distance calls with a calling card. Take your credit card receipt and ATM slips. Shred this information before throwing it away.**
- **Pick up new checks or a reissued credit card at your bank rather than having them delivered to your home. Do not have your driver license number or social security number printed on your checks.**
- **Check your credit report each year for signs of unusual activity.**

- **Limit the exposure of your Social Security number and personal information by giving it only when it is absolutely necessary.**
- **Do Not give your personal information over the phone, over the Internet or through the mail unless you initiated the contact or are certain of the business's trustworthiness.**
- **Keep duplicate records of your wallet's contents.**
- **Mail payments from a safe location. Do not place envelopes in your mailbox where they can be stolen.**

If You Have Been The Victim Of Identity Theft

Contact the Clinton Police Department
(910) 592-3105
Contact the Federal Trade Commission
1-877-IDTHEFT