St. Johns County Sheriff's Office

"Taking Care of People"

Fighting Fraud

How Identity Theft is Committed

- In public places, criminals may engage in "Shoulder Surfing" – watching you from a nearby location as you punch in your Personal Identification Number (PIN) or credit card number.
- Some criminals engage in 'dumpster diving' – going through your garbage cans or commercial dumpsters to obtain copies of your checks, credit cards, bank statements, or other records that may bear your name, address, or telephone number.
- Criminals may simply steal your wallet or purse.
- If you have received applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge.
- Criminals may open up a new credit card account using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They may establish a cellular phone service in your name.
- They may open a bank account in your name and write bad checks on that account.
- Criminals may pilfer bank statements, credit card statements, pre-approved credit card applications, etc, from your mailbox.

Protecting your Identity In Person

- Limit the amount of confidential of personal information you carry in your wallet or purse.
- Avoid carrying more blank checks than you actually need. Do not have your Social Security number pre-printed on your checks.
- Keep good backup information about your accounts, in case your wallet or purse is stolen.
- When you go on vacation, take along a list of toll-free telephone numbers for your banking and credit card companies, not your card numbers, and keep the list in a safe place other than your wallet or purse.
- Consider canceling any credit cards you don't need or haven't used recently.
- Never respond to unsolicited requests for your Social Security Number or financial data.
- Shred credit card applications you receive in the mail and don't use.

- Check all credit card and bank statements for accuracy
- Obtain a copy of your credit report yearly and check it for accuracy
- Be careful of ATM's. 'Shoulder Surfers' can obtain your PIN and get access to your accounts.
- Do not put checks in the mail from your home mailbox. It is easy for someone to change the name of the recipient on the check with an acid wash.
- Obtain a post office box or a locked mailbox if you can.
- Do not put your telephone number on your checks
- Consider an unlisted telephone number or just use an initial instead of full first name in the directory.
- Obtain credit cards and business cards with your picture on them if possible.
- If someone you don't know calls you on the telephone and offers you the chance to receive a "major" credit card, prize or other valuable item, but asks you for personal data such as your Social Security number, credit card number, or mother's maiden name – ask them to send you a written application form. If they won't do it, tell them you are not interested and hang up.
- When you are traveling, have your mail held at your local post office, or ask a neighbor you know well and trust to collect and hold your mail while you are away.
- When you expect a new or replacement credit card in the mail, and it does not arrive, call the card company to see if it was sent. Also make certain no one filed a change of address.
- If your monthly credit card or bank statements do not arrive at the normal time of the month, call the financial institution or credit card company immediately and ask why. Again make certain no one filed a change of address.

Protecting your Identity Online

- In any transaction you conduct, make sure to check with your state or local consumer protection agency and the Better Business Bureau (BBB) to see if the seller, charity, company, or organization is credible. Be especially wary if the entity is unfamiliar to you. Always call the number found on a website's contact information to make sure the number legitimately belongs to the entity you are dealing with.
- Credit cards are the safest way to pay for online purchases because you can dispute the charges if you never get the goods or services or if the offer was misrepresented.
- Crooks pretending to be from companies you do business with may call or send an email, claiming they need to verify your personal information. Don't provide your credit card or bank account number unless you are actually paying for something and know who you are sending payment to. Your social security number should not be necessary unless you are applying for credit. Be especially suspicious if someone claiming to be from a company with whom you have an account asks for information that the business already has.
- Don't send sensitive information such as credit card numbers by email because it's not secure. Look for clues about security on Web sites. At the point where you are asked to provide your financial or other sensitive information, the letters at the beginning of the address bar at the top of the screen should change from "http" to "https" or "shttp." Your browser may also show that the information is being encrypted, or scrambled, so no one who might intercept it can read it.

But while your information may be safe in transmission, that's no guarantee that the company will store it securely. See what Web sites say about how your information is safeguarded in storage.

- Be cautious about unsolicited emails. They are often fraudulent. If you are familiar with the company or charity that sent you the email and you don't want to receive further messages, send a reply asking to be removed from the email list. However, responding to unknown senders may simply verify that yours is a working email address and result in even more unwanted messages from strangers. The best approach may simply be to delete the email.
- Legitimate companies and charities will be happy to give you time to make a decision. It's probably a scam if they demand that you act immediately or won't take "No" for an answer. Some scammers may also demand you pay off a loan immediately or damaging consequences may occur, always take time to look into who is requesting the money before you pay up.
- If someone claims that you can earn money with little or no work, get a loan or credit card even if you have bad credit, or make money on an investment with little or no risk, it's probably a scam. Oftentimes, offers that seem too good to be true, actually are too good to be true.
- A legitimate seller will give you all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty. Contact the seller if any of these details are missing, if they are unable to provide the details, it may be a sign that it's a scam.

Already a Victim of Identity Theft?

If you have been the victim of identity theft, take the following measures:

- In dealing with authorities and financial institutions, keep a log of all conversations, including dates, names and phone numbers. Keep copies of all correspondence. Confirm conversations in writing. Send correspondence by certified mail – return receipt requested.
- File a report with your local law enforcement agency providing as much documented evidence as possible. Obtain a copy of the report and the name/telephone number of your fraud investigator. Provide it to your creditors and others who require verification of your case.
- Immediately contact the three credit reporting companies.

Experian	Equifax	Trans Union Corp
P.O. Box 2104	P.O. Box 105873	P.O. Box 34012
Allen, TX 75013	Atlanta, GA 30348	Fullerton, CA 92834
800-525-7195	800-525-6285	800-680-7286
www.experian.com	www.equifax.com	www.tuc.com

- Contact all creditors immediately with whom your name has been fraudulently used – by phone and in writing. Obtain replacement cards with new account numbers for those that have been fraudulently used. Ask that old accounts be processed as "account closed at consumer's request." Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report such activity immediately to credit grantors.

- If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks you are unsure of. Cancel your checking and saving accounts and obtain new account numbers.
- If your ATM card has been stolen or compromised, obtain a new card, account number, and PIN. Do not use your old PIN. When creating a PIN, don't use common numbers like the last four digits of your SSN or your birth date, and DO NOT WRITE IT DOWN.
- Call the Social Security Administration to report fraudulent use of your social security number at 800-269-0271. As an absolutely last resort, you might want to change your social security number. The SSA will only change it if you fit their fraud victim criteria. Order a copy of your Social Security Earnings and Benefits Statement and check it for accuracy at 800-772-1213.

For more information, contact the Federal Trade Commission: www.consumer.gov/idtheft