St. Johns County Sheriff's Office

"Taking Care of People"

Fighting Fraud – Identity Theft

Identity (ID) theft is a crime where a thief steals your personal information, such as your full name or Social Security number, to commit fraud. The identity thief can use your information to fraudulently apply for credit, file taxes, or get medical services.

These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you are the victim of ID theft until you experience a financial consequence (mystery bills, credit collections, denied loans) down the road from actions that the thief has taken with your stolen identity.

There are several common types of identity theft that can affect you:

- **Child ID theft** - Children's IDs are vulnerable because the theft may go undetected for many years. By the time they are adults, the damage has already been done to their identities.
- **Tax ID theft** - A thief uses your Social Security number to falsely file tax returns with the Internal Revenue Service or state government.
- **Medical ID theft** - This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number to get medical services, or to issue fraudulent billing to your health insurance provider.
- **Senior ID theft** - ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are in more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities that have access to personal information or financial documents.
- **Social ID theft** - A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

Take steps to protect yourself from identity theft:

- Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.
- Don't respond to unsolicited requests for personal information (your name, birthdate, Social Security number, or bank account number) by phone, mail, or online.
- Contact the three credit reporting agencies to request a freeze of your credit reports.
- Collect mail promptly. Place a hold on your mail when you are away from home for several days.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Enable the security features on mobile devices, especially if you have contacts, banking websites and applications saved.
- Update sharing and firewall settings when you're on a public wi-fi network. Consider using a virtual private network, which can give you the privacy of secured private network.

- Review your credit card and bank account statements. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- Shred receipts, credit offers, account statements, and expired credit cards, to prevent “dumpster divers” from getting your personal information.
- Store personal information in a safe place.
- Install firewalls and virus-detection software on your home computer.
- Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases
- Review your credit report once a year to be certain that it doesn't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.

If your identity has been stolen, you can now report your case directly to the Federal Trade Commission online at identityTheft.gov or by phone at 1-877-438-4338. You can also file a report locally with the St. Johns County Sheriff’s Office.

You may also report specific types of identity theft to other federal agencies.

- Medical Identity Theft - Contact your health insurance company’s fraud department or Medicare’s fraud office.
- Tax Identity Theft - Report this type of ID theft to the Internal Revenue Service and your state’s Department of Taxation or Revenue.

In addition to federal government agencies, you should also report the theft to other organizations, such as:

- Credit Reporting Agencies - Contact one of the three major credit reporting agencies to place fraud alerts or freezes on your accounts so that no one can apply for credit with your name or social security number. Also get copies of your credit reports, to be sure that no one has already tried to get unauthorized credit accounts with your personal information. Confirm that the credit reporting agency will alert the other two credit reporting agencies.
- National Long-Term Care Ombudsman Resource Center - Report cases of identity theft that resulted from a stay in a nursing home or long-term care facility.
- Financial Institutions - Contact the fraud department at your bank, credit card issuers and any other places where you have accounts.
- Retailers and Other Companies - Report the crime to companies where the identity thief opened credit accounts or even applied for jobs.
- State Consumer Protection Offices or Attorney General - Your state may offer resources to help you contact creditors, dispute errors and other helpful resources.