Identity theft, as defined by federal law, occurs when someone uses or attempts to use the private personal information of another person to commit fraud. A wide range of information constitutes personal private information, including a person's name, address, Social Security number, date of birth, driver's license number, credit and bank account numbers, and even biometric data like fingerprints.

Red Flags

These warning signs may indicate that identity theft has occurred:

- Suspicious withdrawals or charges on bank or credit statements;
- A notice that personal information was compromised in a data breach;
- A warning from a bank or creditor indicating unusual account activity;
- Errors in a credit report, such as an unknown loan or account;
- A bill for products or services that were never ordered or received;
- A tax return rejected by the IRS because it was already submitted or because reported income does not match IRS records; or
- Calls from a debt collector regarding an unknown debt.

Florida Attorney General's Office
Scams at a Glance:
Identity Theft

Visit MyFloridaLegal.com to find consumer tips or to file a complaint.

Report fraud by calling
1-866-9-NO-SCAM
(1-866-966-7226)

View other Scams at a Glance resources at:
MyFloridaLegal.com/ScamsAtAGlance

Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399-1050

MyFloridaLegal.com

Scams at a Glance:

Identity Theft

OFFICE OF ATTORNEY GENERAL

JAMES UTHMEIER

SAFE ★ STRONG ★ FREE

Stop Identity Theft in its Tracks

Keeping personal information safe, both online and offline, is key to guarding against identity theft. Consider the following tips to protect privacy:

- Create strong passwords using a mixture of upper-case and lower-case letters, numbers, and special characters;
- Never use the same password across multiple websites or apps;
- Use strong security questions. Avoid using questions with answers that are easily guessed or a matter of public record;
- Limit the number of companies that possess personal information. Before signing up with a service, weigh the benefits against the amount of private information that is requested;
- Enable multi-factor authentication whenever possible;
- Do not use public wireless networks to perform financial transactions;
- Check account statements regularly to ensure there are no fraudulent charges;
- Take sensitive outgoing mail to a post office location rather than placing in the home's mailbox;
- Do not provide private information to an unsolicited request received over the phone or via, text, email, or social media messaging;

- Be cautious when posting information or photos to social media feeds;
- Consider placing a credit freeze with each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion) so no new accounts can be opened;
- Check credit reports for fraud at AnnualCreditReport.com at least annually; and
- Shred or safely burn documents that contain personal information prior to disposing of them.

Recover From Identity Theft

Upon discovering that identity theft has occurred, take the following steps:

- File a report with law enforcement;
- Report the incident to the fraud department of each of the three major credit bureaus;
- Report the incident to the fraud department of each creditor, account holder, and financial institution and close accounts that may have been compromised; and
- File an Identity Theft Affidavit with the Federal Trade Commission at IdentityTheft.gov.

Anyone who encounters identity theft should contact the Florida Attorney General's Office at MyFloridaLegal.com or at 1-866-9-NO-SCAM (1-866-966-7226).