Identity Theft Consumer Resource Guide

ATTORNEY GENERAL
LEX
STATE OF FLORIDA

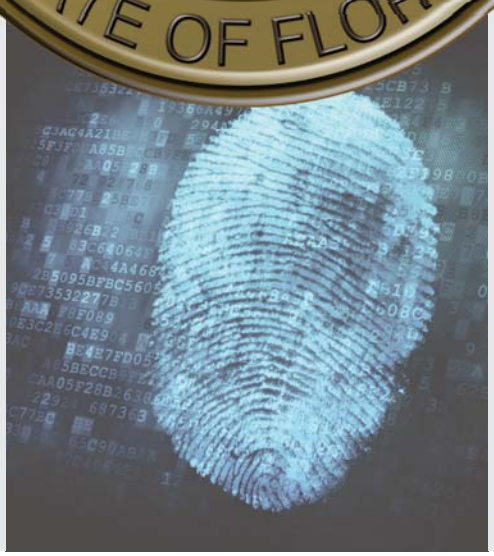


Table of Contents

Dear Fellow Floridians,

According to Consumer Sentinel Network, the state of Florida was the top source in the nation for fraud and scam complaints and the second highest source of identity theft complaints per capita in 2016.

As technology advances, it offers greater opportunities and convenience for consumers and businesses alike. However, it also creates more opportunities for cybercriminals to target Floridians. Meanwhile, identity thieves continue to use offline methods, such as stealing mail and phishing phone calls, to steal personal information.

My office has created this guide to provide you with the helpful information and tools you need to protect against a data breach and avoid becoming a victim of identity theft. It also offers steps to take if you become the victim of identity theft.

I encourage you to contact my office at ***1-866-9-NO-SCAM (1-866-966-7226)*** or online at ***www.MyFloridaLegal.com*** if you have any questions about this guide or if you have been the victim of identity theft. We are here to serve you.

Sincerely,

Pam Bondi

Pam Bondi
Florida Attorney General

Identity Theft

Personal information stolen both online and offline can be used to commit identity theft.

What Is Identity Theft?

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

Identity Theft Warning Signs

Red flags that indicate your identity has been stolen include:

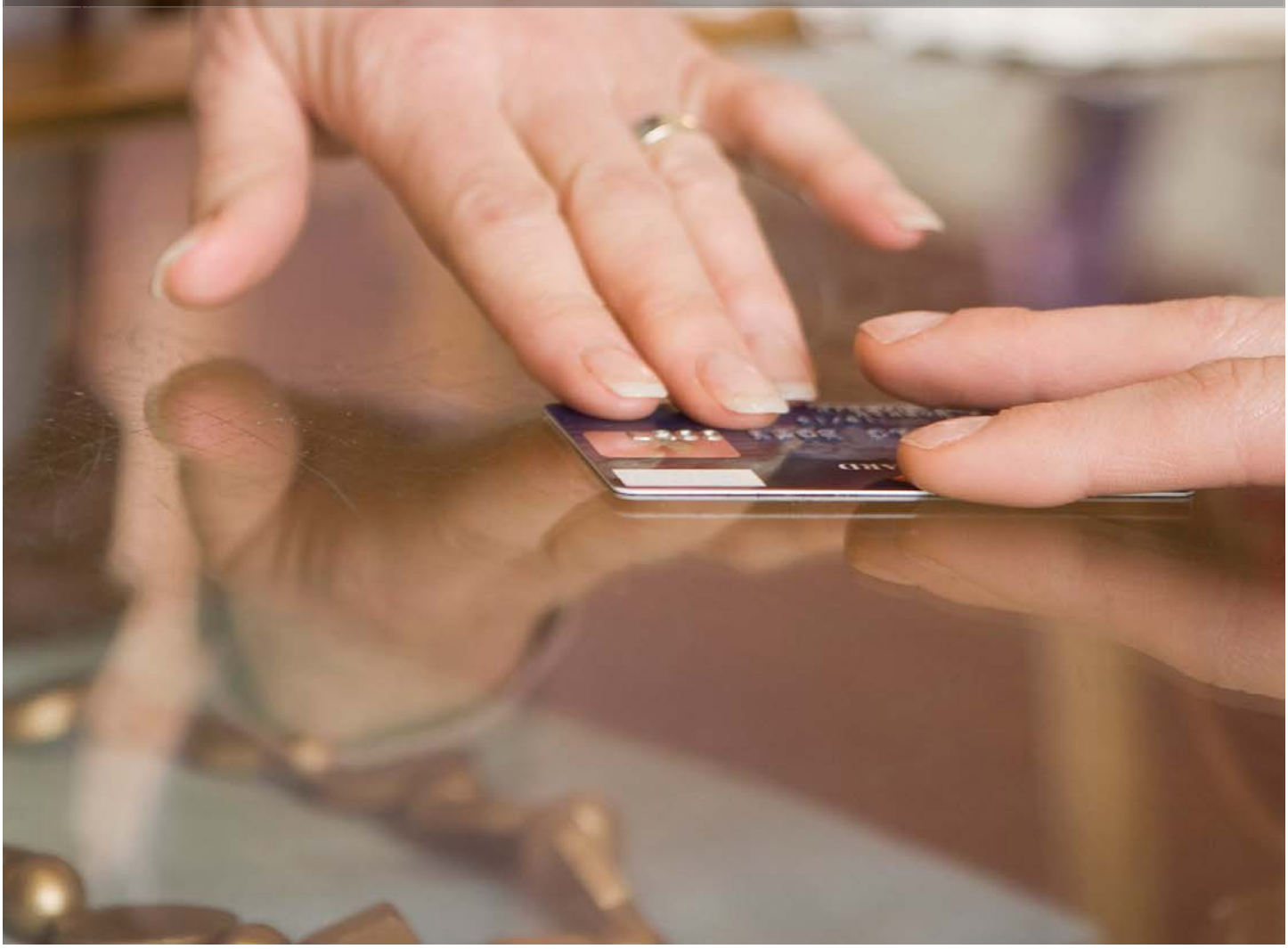
- Being denied access to credit;
- Finding suspicious charges on bank or credit card statements;
- Receiving notice that private personal information has been compromised in a data breach;
- Receiving notice from a bank or creditor indicating suspicious account activity has occurred;
- Noticing that someone has fraudulently forwarded your mail or that you have stopped receiving credit card bills;
- Finding errors in a credit report, such as a loan or account not opened by you;
- Encountering issues with medical insurance, such as a denial of coverage or receiving bills for a treatment never performed;
- Receiving a bill for products or services that were never ordered or never received;
- Being denied state or federal benefits because you are listed as already having received them;
- Having a tax return rejected by the IRS because the refund has already been claimed or the reported income does not match IRS records; or
- Receiving calls from a debt collector regarding a debt not owed.

"According to Consumer Sentinel Network, the state of Florida was the top source in the nation for fraud and scam complaints and the second highest source of identity theft complaints per capita in 2016.

My office has created this guide to provide you with the helpful information and tools you need to protect against a data breach and avoid becoming a victim of identity theft. It also offers steps to take if you become the victim of identity theft.

I encourage you to contact my office at 1-866-9-NO-SCAM (1-866-966-7226) or online at www.MyFloridaLegal.com if you have any questions about this guide or if you have been the victim of identity theft."

-Florida Attorney General Pam Bondi



Tax Identity Theft

For the past six years, tax identity theft has been the most common form of identity theft reported to the Federal Trade Commission.

What Is Tax Identity Theft?

Tax identity theft occurs when someone other than the taxpayer files a fraudulent return using the taxpayer's Social Security number and personal information to receive a refund; fraudulently uses a taxpayer's Social Security number to get a job, causing problems for the victim when his or her income does not match what has been reported to the Internal Revenue Service (IRS); or fraudulently claims a taxpayer's child as a dependent, preventing that child from being rightfully claimed as a dependent on the taxpayer's annual return. Tax identity thieves may access personal information by going through trash cans in search of bills and documents containing sensitive information, posing as the IRS claiming to be contacting the individual about an issue with a tax return, or posing as a legitimate tax preparer for the purpose of accessing personal information.

Protect Against Tax ID Theft

Consumers should take the following steps, as applicable, to safeguard against tax-related identity theft:

- File tax returns as early in the tax season as possible;
- Research a tax preparer thoroughly before providing personal information;
- Use a secure internet connection if filing electronically. Do not use unsecure, publicly available Wi-Fi hotspots;
- Mail paper tax returns directly from the post office, not from home;
- Know that Floridians are eligible for an Identity Protection PIN from the IRS. Should someone enrolled in the IRS IP PIN program and file a return with an incorrect PIN, the IRS will reject or delay the return until the taxpayer's identity can be confirmed. To obtain an IRS IP PIN, visit ***www.IRS.gov*** and search for "IP PIN;"
- Know that the IRS will never initiate contact by email, phone, text or social media. If the IRS needs information, it will do so by U. S. mail; and
- Contact the IRS ID Theft Protection Specialized Unit at ***1-800-908-4490*** if a Social Security number has been compromised.

Child Identity Theft

Many parents and guardians monitor their own credit reports. However, few request their child's credit report, which could result in child's identity theft going undiscovered for years.

What Is Child Identity Theft?

Child identity theft occurs when someone uses or attempts to use a minor's personal information to commit fraud, typically for economic gain. An identity thief may use the minor's information to get a job, sign up for government benefits, gain access to medical care, apply for a loan or open a credit account. Children are particularly at risk for identity theft because there is currently no other credit history associated with their Social Security numbers. This allows criminals to more easily create fraudulent identities using the stolen information. Even more enticing to criminals: A child's stolen identity may not be discovered for years until the child turns 18 and applies for an apartment, student loan or their first credit card.

Child Identity Theft Warning Signs

Red flags that a child's identity may have been stolen include receiving:

- Phone calls or letters attempting to collect debt in a child's name;
- Pre-approval or other credit card offers for minors;
- Notices from a government entity addressed to a child about a traffic violation, jury duty summons, overdue taxes or other such document;
- Bills or insurance claims for medical treatments that the child never received;

- Denial of state or federal benefits because the Social Security number is listed as already receiving those benefits; or
- Notification from the IRS that a dependent cannot be claimed on a tax return because the Social Security number already appears on someone else's tax form.

Check the Child's Credit Report

It is a good idea to check a minor's credit report yearly, particularly while there is still time to dispute and eliminate errors before the child turns 18. Contact each of the three major credit reporting agencies and request a search to see if the child has a credit report on file with them. In addition to asking for the child's credit report, ask each company to perform a manual search based only on the child's Social Security number. This way, if the child's Social Security number is associated with a different name and personal information, it will be discovered. The three major credit bureaus can be contacted at:

Equifax
1-800-685-1111
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-888-4213
www.transunion.com

Parents and guardians will need to provide proof that they are, in fact, the child's parent or legal guardian before the credit reporting agencies will release the minor's credit report. The agencies may require copies of the following documents:

- The child's Social Security number;
- The parent or guardian's government-issued identification card;
- The child's birth certificate listing the requesting adult as a parent or court documents proving the requesting adult is the child's legal guardian; and
- Proof of home address, such as a utility bill, credit card statement or insurance policy.

Keeping IDs Safe (K.I.D.S.) Act

Effective as of September 1, 2014, the K.I.D.S. Act made it possible for a parent or legal guardian in the State of Florida to place a security freeze on the credit report of a child under the age of 16. Parents or legal guardians may place the security freeze on the child's credit report with each of the three major credit reporting agencies. The three agencies can charge a fee not to exceed $10 for the placement or removal of a security freeze. If the child has been a victim of identity theft, there is no cost to place the security freeze.

To place a security freeze on a minor child's credit report: Parents or guardians may be required to provide the following:

- The child's complete name;
- The child's current mailing address;
- The child's previous addresses for the past two years;
- A copy of the child's Social Security card; and
- An official copy of the child's birth certificate

Parents and guardians will need to provide proof that they are, in fact, the child's parent or legal guardian before the credit reporting agencies will place the security freeze on the minor's credit report. The reporting agencies may also require copies of the following documents:

- The parent or guardian's government-issued identification card;
- The child's birth certificate listing the requesting adult as a parent or court documents proving the requesting adult is the child's legal guardian; and
- Proof of home address, such as a utility bill, credit card statement or insurance policy.

Requests must be submitted in writing to each of the three credit reporting agencies at:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Protected Consumer Freeze
P.O. Box 380
Woodlyn, PA 19094

Medical Identity Theft

While most people associate identity theft with stolen credit card numbers and unauthorized loans, identity theft can and does occur in the medical field as well.

What Is Medical Identity Theft?

Medical identity theft occurs when someone uses or attempts to use another person's name and insurance information to receive medical treatment or acquire prescription drugs. Medical identity theft can also occur when someone working in the medical field uses another person's information to submit fraudulent bills to insurance providers.

Medical Identity Theft Warning Signs

Red flags that indicate medical identity theft may have occurred include:

- Receiving a bill for medical treatment or services that were never performed;
- Being contacted by a debt collector regarding medical debt not owed;
- Finding medical collection notices on a credit report for treatment or services that were never received;
- Being told by an insurance provider that the maximum limit on benefits has been reached; or
- Being denied coverage for a particular treatment because records indicate the treatment has already been claimed.

Check with Insurance Providers

Patients who believe their medical identity has been stolen should notify their insurance provider. Patients should always review their Explanation of Benefits from their insurance provider and ensure that claims paid by the insurer match the care they received. Verify the name of the care provider, dates of treatment and list of treatment(s) received. Report any discrepancies to the insurer immediately.

Recovering From Identity Theft

After discovering you are a victim of identity theft, there are immediate actions you should take. Keep in mind, always take detailed notes of actions taken.

1. Contact the Police

File a report with law enforcement. Under Florida Statute Section 817.568(18), consumers may file a report in the location where the theft occurred or in the city or county in which they reside. When filing, consumers should provide as much documentation as possible, including copies of debt collection letters, statements showing fraudulent charges, credit reports and any other evidence they may have. Request a copy of the police report. Creditors and credit reporting agencies may request to see it before removing the debts created by the identity theft from their records.

2. Report the Incident to the Fraud Department of the Three Major Credit Bureaus

Consumers should immediately contact the credit bureaus to place fraud alerts on their credit report. Consumers should also order copies of their credit reports to determine whether there are additional fraudulent accounts listed in their names. Contact the three major credit bureaus at:

Equifax

To report fraud: ***1-800-525-6285***

To order a credit report: ***1-800-685-1111***

www.equifax.com

Experian

To report fraud: ***1-888-397-3742***

To order a credit report: ***1-888-397-3742***

www.experian.com

TransUnion

To report fraud: ***1-800-680-7289***

To order a credit report: ***1-800-888-4213***

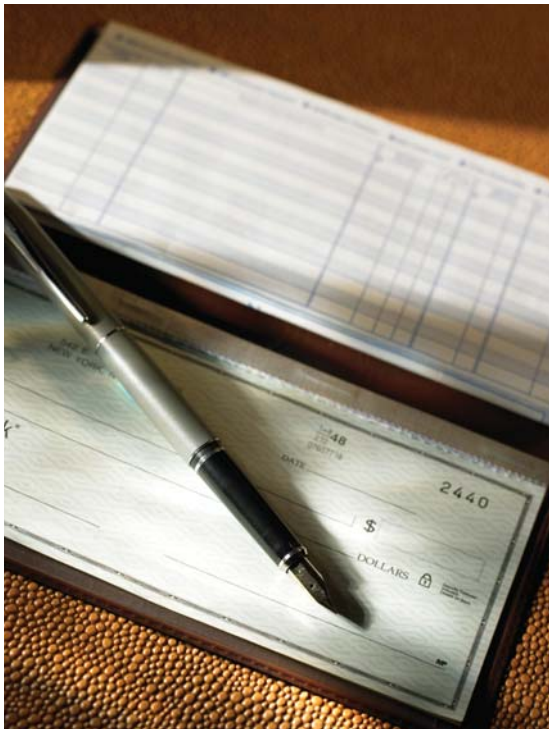
www.transunion.com

3. Contact the Fraud Department of Each Creditor

Consumers should gather the contact information for each of their credit accounts (credit cards, retail credit accounts, utilities, cable and Internet providers, etc.) and call the fraud department for each. Report the incident to each creditor, even if the account at that institution has not been affected. Consumers should close accounts they believe may have been compromised. Request that creditors place an alert on any accounts that remain open. Follow up in writing.

4. File an Identity Theft Affidavit

The Federal Trade Commission (FTC) provides a standardized Identity Theft Affidavit and action plan for victims of identity theft at ***www.IdentityTheft.gov***. It is important to complete this form as some creditors will not begin an investigation or remove fraudulent activity from their records until they receive it. Check with each creditor to determine if it accepts this form; if not, request a copy the creditor's fraud dispute form.



5. Contact Banks or Financial Institutions

If consumers suspect their financial accounts have been compromised, they should close their checking and savings accounts. They should also ask that their banks issue new debit card numbers. Put stop payments on any suspicious outstanding checks. Consumers whose checks have been stolen should contact check and account verification companies and request they notify retailers not to accept checks linked to the stolen account. These third-party services allow businesses to determine whether a check is valid. Three such services can be reached at:

TeleCheck

1-800-710-9898

ChexSystems

1-800-428-9623

Certegy Check Services

1-800-262-7771

Other Actions to Take

Consumers should take the following actions, as applicable, to repair and protect their credit:

- **File a complaint with state and federal authorities.** Consumers should file a complaint with the Florida Attorney General's Office using the toll-free fraud hotline at ***1-866-9-NO-SCAM*** or by visiting online at ***www.MyFloridaLegal.com.*** Consumers should also file a complaint with the FTC's Identity Theft Clearinghouse. Complaint information filed with the FTC is entered into a central database, the Consumer Sentinel, which is accessed by local and state law enforcement agencies. Consumers may call the FTC's toll-free hotline at ***1-877-IDTHEFT*** or complete an online complaint form at ***www.ftc.gov/complaint***.

- **Report a lost or stolen Social Security card to the Social Security Administration.** Consumers may determine whether someone is using their Social Security number for work by creating an account and reviewing their Social Security work history at ***www.socialsecurity.gov/myaccount***. Consumers may apply online for a free Social Security replacement card at ***www.ssa.gov/ssnumber***.

- **If passport fraud is suspected, report it to the U.S. Department of State.** Stolen passports should be reported to the Department of State at ***1-877-487-2778***.

- **Place a flag on Florida driver license.** Consumers with a Florida driver license should flag it with the Fraud Section of the Department of Highway Safety and Motor Vehicles. To place a flag, consumers may email ***fraud@flhsmv.gov*** or call ***850-617-2405***.

- **Check for fraudulent Florida criminal records.** In some instances, an identity theft victim may be faced with a criminal record for a crime he or she did not commit. The Florida Department of Law Enforcement (FDLE) can provide a Compromised Identity Review to determine if any arrests have been falsely associated with the victim as a result of identity theft. Those who believe their identities have been compromised should initiate a review by contacting FDLE at: ***http://www.fdle.state.fl.us/cms/Compromised-Identity-Services/CIS.aspx***.

- **Remove personal identifiers from Florida court records.** Florida law requires the courts to redact personal identifiable information, such as a person's Social Security number, bank account number, credit or debit card number from any public records request. If you believe your personal information appears in a publicly available record, contact your County Clerk's Office. For more information, check the State of Florida Clerk Directory for each county's contact information at ***www.flclerks.com***.

- **Report mail theft to the U.S. Postal Inspection Service.** The U.S. Postal Inspection Service will investigate if a consumer's mail has been stolen by an identity thief. Incidents should be reported to the U.S. Postal Inspection Service. Consumers may file a complaint online at ***http://ehome.uspis.gov/mailtheft/idtheft.aspx***.

Limits on Financial Loss Resulting from Identity Theft

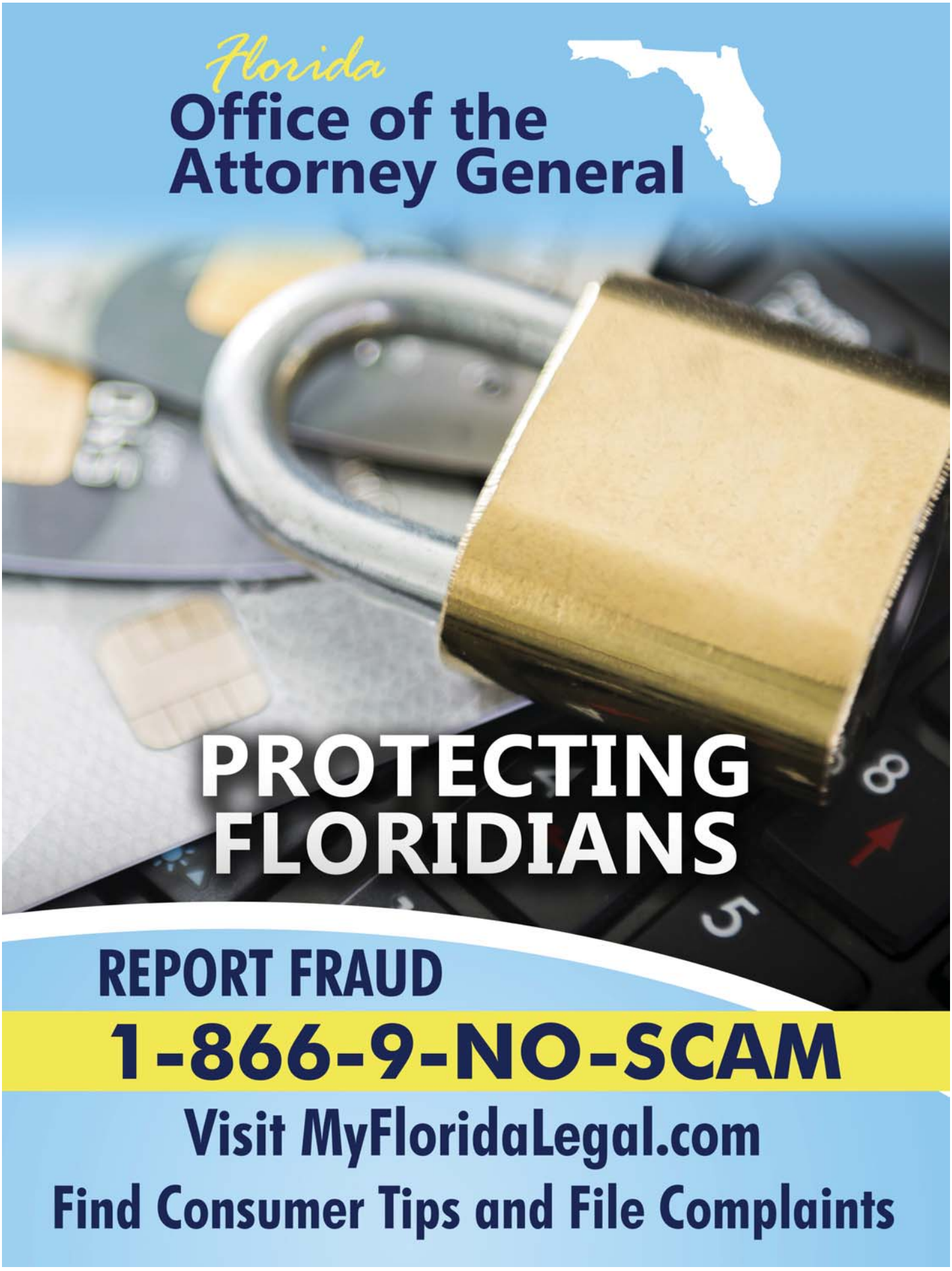
Both federal and state laws limit an identity theft victim's financial losses. Under state law, no identity theft victim may be held liable for any unauthorized charges made on a credit card that is issued without the cardholder's knowledge. Under federal law, the amount an identity theft victim must pay for unauthorized credit card charges is limited to $50. If a victim reports the identity theft prior to unauthorized charges being made, the victim is not responsible for any charges. Under federal law, the amount an identity theft victim must pay for unauthorized charges made on an ATM or debit card varies based upon how quickly the loss is reported.

- If a victim reports the loss or theft of an ATM or debit card prior to unauthorized charges being made, the victim is not liable for any losses.
- If a victim reports the loss or theft within two business days of learning of it, the maximum loss is $50.
- If a victim reports the loss or theft more than two business days after learning of it but fewer than 60 calendar days after receiving a bank statement, the victim's maximum loss is $500.
- If a victim reports the loss or theft more than 60 calendar days after receiving a bank statement, the maximum loss is potentially unlimited.

If an unauthorized charge is made to a victim's bank account using the victim's debit card number but not the physical debit card, the victim is not responsible for the unauthorized charges as long as it is reported within 60 calendar days of receiving a bank statement on which the charges first appear.

Individual financial and credit institutions may waive a victim's responsibility for unauthorized charges as a benefit to their members and cardholders. Consumers should check the terms and conditions of their financial accounts to determine whether they will be held liable for any unauthorized charges.

If an unauthorized charge is made to a victim's bank account using the victim's debit card number but not the physical debit card, the victim is not responsible for the unauthorized charges as long as it is reported within 60 calendar days of receiving a bank statement on which the charges first appear.


Florida
Office of the
Attorney General
PROTECTING
FLORIDIANS
REPORT FRAUD
1-866-9-NO-SCAM
Visit MyFloridaLegal.com
Find Consumer Tips and File Complaints

After a Data Breach

After receipt of a data breach notification, there are immediate actions you should take if the breached entity had access to personal information.

Protecting Your Identity

Consumers should take the following steps, as applicable:

- **Contact the company that suffered the data breach.** Consumers should determine whether the company is offering specific safeguards the consumers can put into place, such as free credit monitoring and/or identity theft protection services.

- **Place a fraud alert on credit reports.** Contact one of the three major national credit reporting agencies and have a fraud alert placed on the report. The agency called is required to notify the other two agencies. A fraud alert means businesses must take extra steps before granting credit in the consumer's name.

  Place a fraud alert at:

  Equifax: ***1-800-525-6285*** or ***www.equifax.com***

  Experian: ***1-888-397-3742*** or ***www.experian.com***

  TransUnion: ***1-800-680-7289*** or ***www.transunion.com***

- **Ask to be issued new card numbers.** If current card numbers have been accessed in a breach, contact creditors to ask for a new card and new card number. If a debit card may have been accessed, request a new card as well as a new account number.

- **Change the password used on the breached company's website.** Consumers who use the same password across multiple websites should change those passwords as well and refrain from using the same password across multiple sites.

- **Consider signing up for a credit or identity-monitoring service.** Sign up for any free monitoring service offered by the breached company. If no monitoring service is offered, research and consider signing up for a service individually.

- **Be wary of emails sent to an email address connected to a breach.** An email address connected to an account that has experienced a breach may see an increase in spam and suspicious email. Consumers who receive suspicious emails should call the business to verify that the email is a legitimate communication. Do not use the number listed in the email to make contact; look up the number on a billing statement, in the phone book or on the entity's website.

- **Consider placing a security freeze on credit reports.** A security freeze is more stringent than a fraud alert. A security freeze is a notice placed on a consumer's credit reports that prohibits the credit reporting agency from releasing the consumer's credit report, credit score or any information within the credit report to a third party without express authorization of the consumer. The agency is authorized, however, to inform the third party that there is a security freeze placed on the consumer's credit report. Once a freeze is in place, the credit reporting agency will mail a confirmation and unique PIN or password that the consumer must use to authorize any changes made to the freeze status. Under Florida law, the credit reporting agencies may charge a fee, not to exceed $10 to place, temporarily lift or permanently lift the security freeze. However, these charges are waived if the consumer is age 65 or older or has been the victim of identity theft and can provide a police report. Place a security freeze with the three major credit reporting agencies at:

Equifax: ***1-800-525-6285*** or
www.equifax.com

Experian: ***1-888-397-3742*** or
www.experian.com

TransUnion: ***1-800-680-7289*** or
www.transunion.com

Protecting Personal Information

Keeping personal information safe, both online and off, is key to guarding against identity theft.

Create Strong Passwords

A strong password is the first step toward protecting against opportunistic hackers who attempt every possible password until they find the correct one. To reduce this threat, consumers should consider the following tips when creating passwords:

- Always change the default password on any account or electronic device.
- Never use "password," "letmein," "qwerty," "12345" or similar easy-to-guess phrases.
- Never use the name of a partner, child or pet; notable dates such as birthdays and anniversaries; the last four digits of Social Security numbers or a favorite sports team or school mascot.
- Use a mixture of upper- and lower-case letters, numbers and special characters. Do not use words found in a dictionary without modifying them with numbers and special characters.
- Ensure all passwords are at least eight characters in length. Generally, the longer the password, the stronger it is.
- Never use the same password across multiple websites.

Use Strong Security Questions

Security questions are often used to reset accounts if the user cannot remember his or her password or must verify the account. Consumers should consider the following tips:

- If presented with a series of possible questions to choose from, pick the one that would be most difficult for someone to guess the answer.
- Avoid picking answers that are public records, can be easily found online or known to friends and family.
- Answer in complete sentences when possible. For instance, if the security question asks for the user's hometown, the answer could be written as, "I was born in Tallahassee, Florida."
- Modify an answer by using numbers and special characters whenever possible. So the user may enter his or her hometown as "T@llaha$$33."

Limit the Number of Companies that Possess Personal Information

The chance that a consumer's personal information could be obtained in a data breach increases with the number of firms that have access to their information. Consider the following tips before providing personal information:

- Before signing up with a service, weigh the benefits of the service against the amount of personal information that is requested.
- When signing up with a particular service, provide only the information that is absolutely necessary. The more personal information a firm has access to, the more information there is that would be lost if that firm experiences a data breach.
- Always read privacy statements to determine how personal information will be used and whether it will be sold to third parties.
- Before sharing personal information such as a Social Security number at the workplace, a business, a school or a doctor's office, consumers should ask why it is needed, how it will be secured and the consequences if not provided.

Additional Tips to Secure Data

Consider these additional tips to guard against data breaches:

- Enable two-factor authentication whenever possible. Companies may allow a user to provide an additional email address or cellphone number where they will send a code to verify that the user is attempting to access his or her account.
- Be cautious about sharing on social media. Consider keeping accounts private and never post information such as account numbers, addresses or phone numbers.
- Some credit card providers offer one-time card numbers to be used for online transactions to further protect consumer financial information. Consumers should contact their provider to see if they have access to such a service.
- Never include personal financial information in an email.

Protect Information Online

For additional methods to remain secure online, consider the following:

- When ordering something online, look to ensure that the browser has a secure connection. In the address bar, a padlock should appear if the browser is secure.
- Know that a financial institution will never email account holders a link for them to "confirm" their account number or "verify" their log-in details.
- Ignore pop-up windows that say the computer has a virus or is infected with malware.
- Do not use public wireless networks, such as those available in hotels or coffee shops, to perform financial transactions.
- Install anti-virus and anti-spyware software on computers.

- Ensure a computer's operating system and web browser are up to date. Change settings so these updates are applied automatically.

Protect Information Offline

For additional methods to remain secure offline, consider the following:

- Read account statements regularly to ensure there are no fraudulent charges.
- Lock documents and records in a safe place at home or in a safe deposit box at the bank. Keep personal information, credit and debit cards and checks secure from guests or workers who come into the home.
- Limit cards carried. Bring only the identification, credit and debit cards necessary. Do not keep your Social Security card in your wallet.
- Consider opting out of prescreened and preapproved offers from credit card companies and other firms. You may opt out permanently or for a period of five years, and may opt back in at any time. To opt out, visit ***www.optoutprescreen.com*** or call ***1-888-5-OPT-OUT***.
- Register your landline and mobile phone numbers on the national Do Not Call list at ***www.DoNotCall.gov*** and the Florida Do Not Call list at ***www.FLDNC.com***.
- Consider photocopying your wallet's contents and keep the copies in a safe or safety deposit box. This way if your wallet is stolen, you can know what information was stolen and which companies to contact about canceling cards and closing accounts.
- Destroy the labels on prescription bottles before disposal.
- Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards and similar documents when they are no longer needed.

- Do not respond to emails, text messages or phone calls asking for personal information. If you believe the request could be a legitimate communication from a company with which you do business, contact the company at the phone number listed on their bill or account statement and inquire whether the communication is legitimate.
- Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in the mailbox. Request a vacation hold on mail and newspapers if you will not be home for several days.
- Check credit reports at least once a year. You have the right to a free credit report each year from each of the three major credit reporting agencies. You can request all three reports at once or get one report every four months. To order a credit report, go to ***www.annualcreditreport.com*** or call ***1-877-322-8228***, toll-free.
- Place an active duty alert with the three credit bureaus, if applicable. Under federal law, a deploying servicemember can place an "active duty alert" on his or her credit report at no cost. An active duty alert on a credit report ensures businesses must take extra steps before granting credit in a servicemember's name. Active duty alerts last for one year and can be renewed to match the period of deployment. To place an active duty alert, servicemembers should contact each of the three nationwide credit reporting agencies:

  Equifax: ***1-800-525-6285***

  Experian: ***1-888-397-3742***

  TransUnion: ***1-800-680-7289***

Download a copy of this guide at:
www.myfloridalegal.com/idtheftguide

PL-01 The Capitol
Tallahassee, Florida 32399-1050
(850) 414-3300
www.myfloridalegal.com

March, 2017