

IDENTITY THEFT



www.MyFloridaCFO.com

December 2024

If you fall victim to identity theft because your personal information was stolen by a criminal, it is important to act quickly. Contacting the right agencies and filing necessary reports will help minimize any financial damage. Here are tips to help prevent identity theft and steps to take should it occur.

OBTAINING YOUR CREDIT REPORT

Everyone in the U.S. can get a free online credit report each week from all three nationwide credit bureaus. Visit AnnualCreditReport.com or call **1-877-322-8228** to obtain your free credit report. To ensure no one but you can access your credit information, you will be asked security questions that only you know. AnnualCreditReport.com is the only federally authorized place to get free annual credit reports. Avoid other sites offering free credit reports.

CREDIT BUREAU CONTACT INFORMATION

EQUIFAX

1-800-525-6285

www.equifax.com

EXPERIAN

1-888-397-3742

www.experian.com

TRANSUNION

1-800-680-7289

www.transunion.com



FIRST STEPS

1

Contact the fraud departments of companies where theft occurred and have those accounts closed to prevent further charges. Update your logins, passwords and PINs.

2

Place a free, one-year fraud alert by contacting one of the three credit bureaus listed in this brochure. The bureau chosen must notify the other two to add the alert to your credit report. This alert warns lenders to take extra precautions before issuing new credit in your name. The alert lasts for one year but can be removed earlier upon request. For more details, visit [What to Know About Credit Freezes & Fraud Alerts](#).

3

Get your free credit reports from Equifax, Experian, and Transunion at [AnnualCreditReport.com](#) or call **1-877-322-8228**. Review your reports and take note of any unfamiliar accounts or transactions. This will assist you when reporting identity theft to federal and local authorities.

4

Report identity theft to the [Federal Trade Commission](#) (FTC) at [IdentityTheft.gov](#), including as many details as possible. [IdentityTheft.gov](#) will create a report and recovery plan that you can print. Creating an account allows [IdentityTheft.gov](#) to update your plan, track progress, and pre-fill forms and letters as needed.

5

Report identity theft to your local law enforcement agency. Take your FTC report, photo ID, proof verification of address, and any proof of the theft, like bills or an IRS statement. If the theft occurred in a different city/state, report it to that local jurisdiction. Request a copy of the report for future use in the identity theft recovery process.

PROTECT YOUR PERSONAL INFO



Create secret passwords that are easy for you to remember but difficult for others to guess. Procedures are in place to reset them if you forget.

Do not reuse passwords across accounts and change them regularly. For more info: [FTC Password Checklist](#).



Your passwords should have a minimum of 12-16 characters with upper and /lower-case letters, numbers and include symbols such as an ampersand (&) or hyphen.

Use multi-factor authentication when available for [extra protection](#).



Shred all personal and financial documents that you no longer need.

When traveling, contact the post office to hold your mail and consider dropping bill payments off at the post office or a secure mailbox.



Store sensitive personal documents in a safe place, carrying only what you need. Avoid carrying your Social Security card or writing your number on a check.

Install and maintain an anti-virus program on your computer and delete spam email.



ADDITIONAL TIPS

Be wary of requests that direct you to a website or toll-free number asking for personal information or your password.

If the request or call is from a creditor, do not respond. Instead contact the agency directly using the phone number on your credit card or financial statement.

Avoid sharing personal information over the phone unless you initiated the contact. Ask who will have access to it and how it will be secured.

If a charity calls, determine if they are registered using the [Check-A-Charity tool](#) before you share personal financial information.

Only provide personal information over a secured internet site with will that has "https" and a padlock icon in the URL.

Review your credit reports and bank accounts regularly for suspicious activity and report it immediately.

Go to [FLHSMV.gov](#) (Florida Highway Safety and Motor Vehicles) and request the department to put a 'Verify ID Flag' on your driver's license. If anyone tries to make a change to your driver's license, HSMV must check with you first.

Contact your bank to let them know your ID was stolen. The bank can lock your accounts to ensure no one can electronically remove funds.

To learn more about frauds and scams that target seniors, visit [Be Scam Smart](#).