



REPORT TO THE AUTHORITIES AND CREDIT BUREAUS

When your private financial information gets into the wrong hands, the consequences can be devastating. If you fall victim to identity theft, it is important that you act quickly. Contacting the correct agencies and filing the necessary reports will go a long way toward minimizing any damage to your financial well-being.

Credit Bureaus: Immediately contact the fraud departments of each of the credit bureaus listed on the back of this brochure. Alert them that you are a victim of identity theft, and request that a fraud alert be placed in your file. You can also request a security freeze, preventing credit issuers from obtaining access to your credit files without your permission. This prevents thieves from opening up new credit cards in your name.

Law Enforcement: Report identity theft to your local police department. If the crime occurred somewhere other than where you live, you may wish to report it to law enforcement there as well. The police will create an "identity theft report" and you can request a copy.

Federal Trade Commission (FTC): The FTC does not investigate identity theft cases, but they can share information that you give them, such as the identity theft report number, with investigators nationwide. For more information about fighting back against identity theft, visit the FTC's Identity Theft website at www.consumer.ftc.gov/features/feature-0014-identity-theft. The Federal Trade Commission's Identity Theft Hotline is **877-IDTHEFT (877-438-4338)**. For more information on ways to protect yourself, visit www.MyFloridaCFO.com/YMM/CreditAndDebt/IdentityTheft.



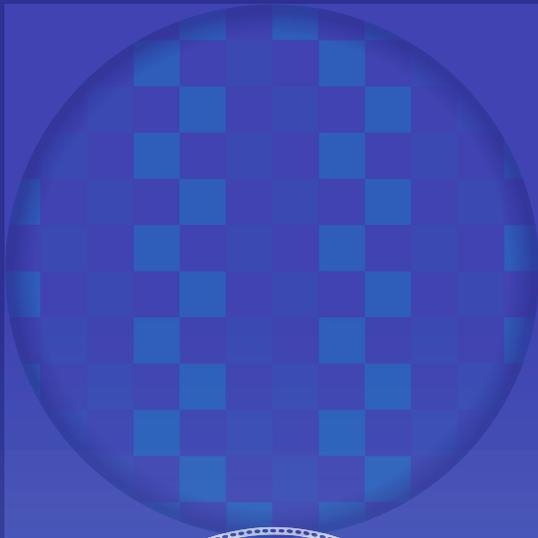
INCREASE YOUR PERSONAL SECURITY

- Create your own secret password. Be creative when mixing numbers, symbols and uppercase letters in your own way.
- Your password should be easy for you to remember, but difficult for anyone else to guess.
- Do not use the same password for all accounts and change your it regularly.
- Immediately change your password if you suspect that someone else may have gained access to it.
- If you forget your password, procedures are in place with your financial institutions and creditors to reset or remind you of your password.
- Preferably, your password should have a minimum of eight characters and at least one symbol that is not a number or letter, such as an ampersand (&) or a percent sign (%).
- Using secure passwords is key to protecting yourself from identity theft. For more information, visit www.MyFloridaCFO.com/YMM.



PROTECT YOURSELF FROM IDENTITY THEFT

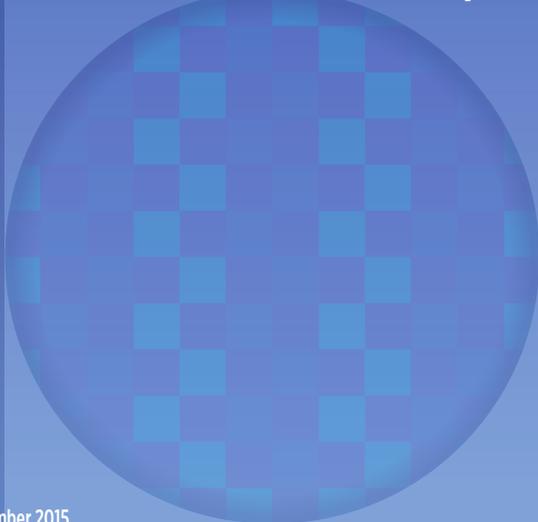
- Be wary of requests that direct you to a website or toll-free number asking for personal information or your password.
- If the request or call is from a creditor, do not respond. Instead contact the agency directly using the phone number on your credit card or financial statement.
- If you are going to be away for an extended period of time, contact your local post office to hold your mail until you return.
- Install and maintain an anti-virus program on your computer.
- Only provide personal information over a secured site; the addresses for these sites will include "https" in your web browser and a padlock icon at the bottom.
- Shred all personal and financial documents that you no longer need.
- Before you share personal information, ask who will have access to it and how it will be secured.
- Knowing how to prevent identity theft is the most important step to avoid being a victim. For more information, visit www.MyFloridaCFO.com/YMM.



CHIEF FINANCIAL OFFICER
JEFF ATWATER
FLORIDA DEPARTMENT OF FINANCIAL SERVICES



WWW.MYFLORIDACFO.COM/YMM



PROTECT YOURSELF AGAINST IDENTITY THEFT

There are some simple steps you can take to reduce or minimize the risk of becoming a victim of identity theft.

PRACTICE SAFE INTERNET USE AND BEWARE OF SCAMS

Always be on the defense with your private information. Delete spam emails that ask for personal information, and keep your anti-virus and anti-spyware software up-to-date. Shop online only with secure web pages (check the bottom of your browser for an image of a lock or look for "https" in the address bar). Never send credit card numbers, Social Security Numbers and other personal information via email or over the phone from someone claiming to represent your bank, credit card issuer, a government agency, a charity or other organization. If you think the request is legitimate, contact the company directly to confirm their claims.

DESTROY PRIVATE RECORDS

Shred credit card statements; ATM, credit or debit card receipts; bank deposit receipts; loan solicitations; and other documents that contain private financial information.

SECURE YOUR MAIL

When mailing bill payments and checks, consider dropping them off at the post office or a secure mailbox.

BE CAREFUL WITH YOUR SOCIAL SECURITY NUMBER (SSN)

Your Social Security Number is a major target for identity thieves because it can give them access to your credit report and bank accounts. Never carry your SSN card with you. Instead, memorize your number and keep the card in a secure place at home or in a safe deposit box. Never write or print your Social Security Numbers on checks.

CHECK YOUR CREDIT REPORT

At least once a year, obtain and review your credit report for suspicious activity. You can request a free copy of your report at www.AnnualCreditReport.com or 1-877-322-8228 or by contacting any one of the three major credit reporting agencies.

CREDIT BUREAU CONTACT INFORMATION

EQUIFAX

Report Order: 1.800.685.1111
Fraud Hotline: 1.888.766.0008
www.equifax.com

EXPERIAN

Report Order and Fraud Hotline:
1.888.397.3742
www.experian.com

TRANS UNION

Report Order: 1.877.322.8228
Fraud Hotline: 1.800.680.7289
www.tuc.com