



## Identity Theft -- don't be left in the dark

A Message from the Commissioner...

Dear Florida Citizens,

*Identity theft is a growing concern for consumers everywhere. Your personal information is needed to conduct business and financial transactions, but this often leaves you vulnerable to criminals. Your personal information can fraudulently be used to obtain credit and services in your name, damaging your credit rating and jeopardizing your financial stability.*

*The Florida Department of Agriculture and Consumer Services has compiled this information to help you prevent and, if it occurs, react to identity theft. We have included informational tips and clear step-by-step instructions on what you can do in the event your personal information is "hijacked" or stolen, and then used.*

*There are simple steps you, as a consumer, can take to secure your privacy. Becoming informed is the very best security you can give yourself to ward off the potential threat of identity theft.*

Sincerely,

Charles H. Bronson  
Commissioner

### The First Signs of Identity Theft

Because of the nature of the crime, victims often do not realize their identity has been stolen until they are denied credit, turned down for a job, or sent a bill for purchases they did not make. Other signs are:

\* You are contacted by a collection agency regarding a debt you did not incur.

\* Checks disappear from your check book.

\* You get a phone call or letter telling you that you have been approved or denied credit for accounts you never requested.

By obtaining your personal information, identity thieves can wreak havoc with your credit, your financial security and your peace of mind.

**Quick Tip** - Keep photocopies of your driver's license, credit cards, Social Security Card, insurance cards and other

contents of your wallet or purse in a secure place.

### It's Your Identity - Keep it Safe

While consumers with high incomes are the preferred prey of identity thieves, every consumer is a potential target. Even though it may be impossible to totally eliminate the chances of becoming a victim of identity theft, there are many preventive steps a consumer can take to insure the security of their financial identity.

1. Order a copy of your credit report from each of the three major credit bureaus, once a year.

2. Mail payments for bills from post office collection boxes. Tear or shred charge receipts, copies of credit applications, insurance forms, physician statements, expired credit cards and credit card offers before discarding into the trash.

3. Store Social Security cards, credit cards, cancelled and extra checks, passports and any additional identity documentation in a secure place.

4. Remove extraneous information such as middle name, phone number, Social Security Number or driver's license number from your checks.

5. Review credit card, telephone, cellular phone and bank statements for irregularities and be aware of your billing cycles. Contact creditors immediately if you find a discrepancy. Close all accounts that are no longer needed or used. Write the company a letter and ask them to verify, in writing that the account has been closed.

6. Use passwords on all your accounts. Avoid picking easily determined numbers such as birth date, mother's maiden name or last four digits of your social security number.

7. Send "opt out" letters to businesses you have a relationship with, restricting them from selling, renting, distributing, or exchanging your personal information. Advise the three major credit bureaus you do not want personal information about

you shared for promotional purposes. To stop receiving pre-approved credit offers call 1-888-5-optout (567-8688) .

### Opting Out

Send opt out letters to: your financial institutions, mortgage company, Direct Marketing Association, telephone company, charities, department stores, other merchants and the three major credit bureaus.

Opting Out Sample Letter:

*To Whom It May Concern:*

*I hereby opt out of the sale, rental, distribution, exchange or other disclosure of any and all personal information you may have about me. This includes, but is not limited to my name, home and work phone numbers, email and home addresses, Social Security numbers, financial account numbers and my transaction history with you.*

*Please promptly confirm in writing that you will not disclose my personal information without my written consent.*

Full Legal Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Address: \_\_\_\_\_

Date: \_\_\_\_\_

Even though other companies may still contact you, sending these companies an opt out letter will lessen the possibility of your private information becoming available to unscrupulous persons

### For Credit Bureaus, write to:

Equifax, Inc. - Options  
PO Box 740123, Atlanta, GA 30374

Experian - Consumer Services  
901 West Bond St., Lincoln, NE 68521

Trans Union - Marketing List Opt Out  
PO Box 97328, Jackson, MS 39288-7328

### For Direct Marketing, write to:

Direct Marketing Association - Mail Preference Association  
PO Box 643, Carmel, NY 10512

**Quick Tip** - In most cases, the Truth in Lending Act limits your liability for unauthorized credit card charges to \$50 per card. The Fair Credit Act establishes procedures for resolving billing errors on your credit card accounts. This includes fraudulent charges on accounts.  
**IMPORTANT:** In order for these laws to be of benefit to you, it is essential the fraud be reported within 60 days.

### What if it Happens to Me?

Both the State of Florida and the Federal Government are great resources for information on identity theft. Contact the Florida Attorney General's fraud line at 1-866-966-7226 or visit them online. To report a crime, call the Federal Trade Commission's toll-free Identity Theft Hotline at 1-877-438-4338. They will provide additional information and give you instructions on what to do next. Ask that an affidavit of fraud to be sent to you immediately.

Call each company that issued a fraudulent credit card to obtain a copy of the signed credit card contract. Be persistent. Ask them to send notification to the three major credit bureaus so they are made aware of the fraud. They may request an affidavit of fraud and a police report.

Contact any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your credit alert, the other two credit bureaus will be automatically notified to place fraud alerts in their system, and all three credit reports will be sent to you free of charge.

### Credit Bureaus

**Equifax**  
To order your report, call: 1-800-685-1111  
To report a fraud, call: 1-800-525-6285  
TDD 1-800-255-0056 and write to:  
P.O. Box 740241, Atlanta, GA  
30374-0241Experian  
To order your report, call: 1-888-397-3742  
To report a fraud, call: 1-888-397-3742  
TDD 1-800-972-0322 and write to:  
P.O. Box 9532, Allen, TX 75013

**TransUnion**  
To order your report, call: 1-800-888-4213  
To report a fraud, call: 1-800-680-7289  
TDD 1-877-553-7803 and write to:  
Fraud Victim Assistance Department  
P.O. Box 6790, Fullerton, CA 92834-6790

At your request, the Fraud Section of the

Florida Department of Highway Safety and Motor Vehicles will place a flag on your driver's license if you are a victim of identity theft (regardless of whether your license has been compromised). To reach the Fraud Section, call 1-800-488-4579. You will be asked to submit your request in writing to: Florida Department of Highway Safety and Motor Vehicles, DDL/BDI - Fraud Section, Room A327, Neil Kirkman Building, Tallahassee, FL 32399-0570

### Other Steps to Take

\* Call SCAN 1-800262-7771 to find out if the identity thief has been passing bad checks in your name. If your checks have been fraudulently used, notify: Global Payments at 1-800-766-2748, Certegy, Inc. at 1-800-437-5120, TeleCheck at 1-800-366-2425, and ChexSystems/Efunds at 1-800-328-5121

\* Report fraudulent use of your Social Security Number to the Social Security Administration. To file a report call 1-800-269-0271, between 10:00AM and 4:00PM Eastern Time.

\* Contact your local office of the Postal Inspection Service if you suspect that an identity thief submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity.

\* Follow up in writing with all contacts you have made on the phone or in person. Use certified mail, return receipt requested. The letter that you send the contact person should simply state what occurred in the telephone conversation or correspondence and what actions were agreed upon.

\* Keep the original copies of any correspondence or documentation that you send.

\* Keep old files even if you believe your case is closed. One of the most difficult and annoying aspects of identity theft is that errors can reappear on your credit reports or your information can be re-circulated. Should this happen, you will be glad you kept your files.

\* Set up a filing system from the very start. Information can become overwhelming very quickly and be impossible to manage.

**Quick Tip** - Don't rely on the mail to deliver checks. If you receive monthly

checks or are expecting money like a tax refund, have the money directly deposited into your bank account. If this is not a possibility, get a post office box specifically for this purpose.

### Mail... What to do When You're Out of Town

If you are planning to be away from your home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold or make the request at your local post office. The Postal Service will hold your mail at your local post office.

### Computer Privacy

There is a risk of identity theft if personal and financial records are stored on your computer. You can greatly reduce the possibility of your financial information becoming another person's identity.

\* Use a firewall program if you use a high speed internet connection that leaves your account connected to the Internet 24 hours a day.

\* Use a secure browser. Some browsers can be downloaded and are free on the Internet.

\* Don't store your financial information on a laptop unless it is absolutely necessary. If you do, set up the pass word with lower and upper case letters and symbols and do not use an automatic log in.

\* Look for Web site privacy policies. If you do not see a privacy policy, consider surfing elsewhere.

\* Delete personal information from any computer being discarded or given away. A full "wipe" is necessary to ensure the deletion of information from the hard drive.

\* Update virus protection software regularly. Viruses can divert your private information or render your information accessible to outsiders if these updates are not preformed.

**Quick Tip** - Most legitimate businesses will not ask you for your Social Security or bank account numbers. If they do, ask if an alternative number can be used.