IDENTITY THEFT AND FRAUD

With Identity Theft and Identity Fraud becoming such a fast growing and serious crime in the United States and Florida, we knew we needed to obtain helpful information for the citizens of DeSoto County. We found numerous articles, bulletins, and publications on the internet from the following agencies: U. S. Federal Trade Commission (FTC), Social Security Agency (SSA), Internal Revenue Service (IRS), U. S. Office of Inspector General (OIG) of the Office of U. S. Department of Education, U. S. Postal Service (USPS), U. S. Department of Justice, Florida Attorney General, Wikipedia.org, and CNN. The following is a summary, and reprint in some instances, from all of those agencies.

Listed below are the various topics regarding identify theft and fraud for your review:

1. WHAT IS IDENTITY THEFT AND IDENTITY FRAUD?
2. HOW IDENTITY THEFT OCCURS.
3. FINDING OUT IF YOU ARE A VICTIM OF IDENTITY THEFT.
4. HOW TO PROVE YOU ARE A VICTIM.
5. TAKING CHARGE BY ORGANIZING YOUR EFFORTS.
6. IMMEDIATE STEPS TO TAKE IF YOU ARE A VICTIM.
7. SPECIFIC PROBLEMS:
   - Bank Accounts
   - Bankruptcy Fraud
   - Correcting Fraudulent Information in Credit Reports
   - Credit Cards
   - Criminal Violations
   - Debt Collectors
   - Driver’s License
   - Investment Fraud
   - Long Distance, Cable, Radio, Satellite, TV and Wire
   - Mail Theft
   - Military
   - Passport Fraud
   - Phone Fraud
   - Scholarships
   - Social Security Number Misuse
   - Student Loans
   - Tax Fraud
8. PRECAUTIONS TO TAKE TO AVOID BECOMING A VICTIM

9. STAYING ALERT

1. WHAT IS IDENTITY THEFT AND IDENTITY FRAUD?

Identity theft and identity fraud are terms used to refer to the deliberate assumption of another person’s identity or the use of another person’s personal data usually to gain access to their finances. It can also include framing them for a crime, enable illegal immigration, terrorism, espionage or changing identity permanently.

In short, identity theft or identity fraud is a crime.

The proper reference to the crime is identity fraud. However, most people refer to it as identity theft.

Identity theft is one of the fastest growing crimes in the United States. Either you or someone you know has probably been a victim of identity theft since one in five people become victims every year.

Victims whose identities have been stolen may spend hundreds of dollars, as well as months and years, trying to straighten out the problems the thieves have caused. Also, the costs to businesses is billions of dollars annually, which is passed on to consumers.

For those reasons, in 1998 Congress created a new federal offense of identity theft entitled “The Identity Theft and Assumption Deterrence Act”. This offense carries a maximum term of 15 years imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense. Under the U. S. Code, schemes to commit identity theft or fraud may involve violations of other statutes that are felonies that carry penalties in some cases as high as 30 years imprisonment. In addition, Florida has enacted F. S. 817.568 entitled “Criminal Use of Personal Identification Information”.

2. HOW IDENTITY THEFT OCCURS.

Identity theft occurs when someone uses your name, Social Security number, birth date, and other personal information without your permission. With this information, an identity thief is only limited by his creativity.

Identity thieves obtain your personal information by some of the following ways:

- Stealing records or information from businesses while they work there;
- Bribing an employee of a business for information;
- Hacking into business records;
- Stealing your mail;
✓ Rummaging through your trash or the trash of businesses, which is known as “dumpster diving”;
✓ Obtain your credit reports by fraudulent means, such as posing as a landlord;
✓ Stealing your wallet, credit or debit cards;
✓ Steal credit or debit card numbers by capturing the information in a data storage devise, which is called “skimming”;
✓ Complete a “change of address card” to divert your mail;
✓ Stealing personal information from you through email or phone by posing as legitimate companies and claiming they have a problem with your account. This is known as “phising” online (pronounced as fishing).
✓ Watching you in public places, from nearby location, as you punch in a calling card number or credit card number or listen in on your conversation which is called “shoulder surfing”.

Unfortunately, the identity thief is often someone previously known to the victim, such as a friend, family member, or acquaintance.

In the U.S., there is much personal information, such as mortgage details, social security numbers, and driver’s license information, that is publicly available. Credit reference agencies hold comprehensive personal financial information and other personal data. Junk mail from these agencies has increased the possibilities of theft and fraud.

In addition, there are many lenders and credit card companies that will extend credit without actual human contact with the borrower. This is done through the mail or by internet.

If the criminal has the bills for falsely obtained credit cards, bank statements, etc., sent to an address other than your address, you may not become aware of the identity theft until substantial damage has occurred to your credit, assets, and reputation.

3. FINDING OUT IF YOU ARE A VICTIM OF IDENTITY THEFT.

You may not know you have become a victim of identity theft until you start receiving bills for accounts you have never opened, you stop receiving bills for accounts you have, you see charges on your accounts that you didn’t authorize, or you stop receiving your bank statements.

If you don’t receive statements or if you receive unexplained bills, call the creditor, phone company, or bank or financial institution immediately to get as much information as you need to determine whether you have become a victim. Checking your monthly statements carefully may be the quickest way for you to find out if you have become a victim.
Beginning September 1, 2005, federal law requires that each of the three major credit bureaus provide one free credit report per year to every person upon request. All you need to do is place a fraud alert on your credit reports. Call the toll-free fraud numbers or contact them by internet or write of any of the following credit bureaus:

Equifax: 1-800-525-6285; www.equifax.com; P. O. Box 740241, Atlanta, Ga. 30374-0241
Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P. O. Box 9532, Allen, Tx. 75013
TransUnion: 1-800-680-7289; www.tuc.com; Fraud Victim Assistance Division, P. O. Box 6790, Fullerton, Ca. 92834.

At your request, the credit bureau will only place the last four digits of your Social Security Number on your credit reports. In addition, all you need to do is contact one of the credit bureaus and that bureau is required to contact the other two, which will place an alert on their reports.

Once you receive your credit reports, review them carefully looking for accounts you didn’t open, or any unexplained debts.

4. HOW TO PROVE YOU ARE A VICTIM.

When you find accounts or credit cards that have been opened in your name that you did not apply for, request, in writing, for copies of the application or other transaction records from the companies that issued the accounts or cards. Companies must provide these records at no charge to you within 30 days of receipt of your request.

Upon examination of the applications you may be able to prove that the signature on the application is not yours, that the address is not yours, or that employment information is incorrect. In addition, the incorrect information may be useful to law enforcement.

Before writing the company, call them as they may request proof of identity, which may be a photocopy (not an original) of a state or government-issued ID card. In addition, you may complete an ID THEFT AFFIDAVIT that has been developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission, which you may download from the following website: www.consumer.gov/idtheft then go to paragraph 2. and click on IDTHEFTAFFIDAVIT. If you do not have access to the internet, you may call the FTC’s Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338). Many companies accept this affidavit, but some may require that you submit more or different forms. Before sending the affidavit, contact each company to find out if they accept it or not.

The ID Theft Affidavit has two parts:
   Part One – the ID Theft Affidavit – this is where you report general information about yourself and the theft.
Part Two – the Fraudulent Account Statement – which is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

Be sure you attach copies of any supporting documents, such as driver’s license, police report, etc.

After completing the affidavit, mail a copy to each creditor, bank, or company that provided the identity thief with the unauthorized credit, goods, or services you describe, by certified mail, return receipt requested, so you can prove your affidavit was received. Keep a copy of everything you submit. Completing the affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

5. TAKING CHARGE BY ORGANIZING YOUR EFFORTS.

Having complete and accurate records of your efforts will help you to resolve your identity theft quicker.

Here are some tips:

✓ When you contact a company, don’t assume the person you talk to will give you all the information you need. Prepare a list of questions you may have for them or information you wish to relay to them. Do not hang up until you understand everything they tell you.
✓ Write down the names of everyone you talk to, what they tell you, and the date of the conversation. (See the Chart below.)
✓ Follow up in writing with all companies you contact. Send your letter by certified mail, return receipt requested, so you have a record of what the company received and when.
✓ Keep copies of all correspondence or forms you send.
✓ Keep copies of all correspondence or forms you receive, including the envelopes.
✓ Keep originals of all police reports and other documents you obtain in a safe place. Only send copies to the creditors, banks, credit bureaus, etc.
✓ Keep all of your records even if you believe your case is closed. Most cases stay resolved, but problems can come up later.

Following is a sample of a Chart for keeping track of your contacts:

<table>
<thead>
<tr>
<th>Contact, Credit Bureau or Agency</th>
<th>Address or Phone Number</th>
<th>Date Contacted</th>
<th>Contact Person</th>
<th>Report or Confirmation Number</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. IMMEDIATE STEPS TO TAKE IF YOU ARE A VICTIM.

**FIRST:** Place a fraud alert on your credit reports. This can help prevent an identity thief from opening any more accounts in your name. Contact the following credit bureaus by phone, internet, or writing:

- **Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P. O. Box 740241, Atlanta, Ga. 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P. O. Box 9532, Allen, Tx. 75013
- **TransUnion:** 1-800-680-7289; [www.tuc.com](http://www.tuc.com); Fraud Victim Assistance Division, P. O. Box 6790, Fullerton, Ca. 92834

There are two types of fraud alerts: an initial alert and an extended alert. The initial alert stays on your credit report for at least 90 days. The extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you have been a victim of identity theft and you provide the consumer reporting company with an ID Theft Affidavit or their identity theft report. An extended alert on your credit report entitles you to two free credit reports within twelve months from each of the three credit bureaus. In addition, the credit bureaus will remove your name from marketing lists for companies and from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the lists before then.

To place either alert on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity.

When a business sees the alert on your credit report, they must verify your identity before issuing you credit. The business may try to contact you directly, which may cause some delays if you are trying to obtain credit. You may wish to include a cell phone number in your alert where you can be reached easily. Remember, keep all contact information current in your alert.

**SECOND:** Close all accounts that you know, or suspect, have been tampered with or opened fraudulently. Call and speak with someone in the security or fraud department of each company and follow up in writing. Send all letters and copies of supporting documents by certified mail, return receipt requested, so you have proof what the company received and when. Keep a copy of all letters and documentation for your records.

Ask the company for their fraud dispute forms to dispute any fraudulent charges or accounts opened without your authorization if they do not accept the ID Theft Affidavit. In addition, use the following sample letter to dispute the fraudulent charges or opened accounts:
Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $__________. I am a victim of identity theft, and I did not make this (charge or debt). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report, ID Theft Affidavit) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

(Your signature)
Your printed name

Enclosures: (List what you are enclosing.)

Be sure and address your letter to the address given for “billing inquiries”, NOT the address for sending your payments.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed account(s) and has discharged the fraudulent debts. This letter is your best proof of error relating to this account reappearing on your credit report or if you are contacted again about the fraudulent debt.

THIRD: File a report with your local law enforcement or law enforcement in the community where the identity theft took place. In Florida, fraudulent use of personal identification information is a violation of F. S. 817.568. Anyone who violates any of the various subsections under this statute is committing an offense, which can range from a misdemeanor of the first degree to a felony of the first degree.
After filing a report, get a copy of the report so you can forward copies of it to the creditor(s) that need proof of the crime. If the law enforcement agency is reluctant to take your report, ask to file a “Miscellaneous Incidents” report.

If you still have a problem getting a report, you may contact the Florida Attorney General toll-free at: 1-866-966-7226.

In addition to contacting local law enforcement, you may need to contact the following federal agencies:

**Department of Justice (DOJ) @ www.usdoj.gov** You may get more information @ www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud to have the U.S. Attorney prosecute.

**Federal Bureau of Investigation (FBI) @ www.fbi.gov** They investigate cases involving bank fraud, mail fraud, wire fraud, bankruptcy fraud, insurance fraud, fraud against the government, and terrorism.

**U. S. Secret Service (USSS) @ www.secretservice.gov** They investigate financial crimes if the dollar loss is substantial.

**FOURTH:** File a complaint with the Federal Trade Commission. You can file the complaint using the online complaint form at the following website: www.consumer.gov/idtheft then go to Paragraph 4. and click on “File Your Complaint with FTC”, or you may contact the Identity Theft Hotline toll-free at 1-877-IDTHEFT (438-4338); or by mail to the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you obtain additional information or problems. Be sure and keep them informed of any changes in your mailing address and telephone number.

The Federal Trade Commission publishes free brochures on identity theft and many consumer issues. For a complete list of free publications, write for Best Sellers, Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or call toll-free 1-877-FTC-HELP (382-4357); or log on to http://www.ftc.gov/ftc/consumer.htm.

By filing your identity theft complaint with the Federal Trade Commission, you will provide important information that can help law enforcement track down identity thieves and stop them.

7. **SPECIFIC PROBLEMS**

**Bank Accounts:** State laws protect you against fraud committed by a thief using stolen or counterfeit checks. But if they used an electronic fund transfer, federal law applies. If
you are not sure what type transaction the thief used, ask the financial institution that processed the transaction.

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card, or another electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

You have 60 days from the date your bank account statement is sent to you to report, in writing, any money withdrawn from your account without your permission.

If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss.

If you report the loss or theft within two business days of discovery, your losses are limited to $50.00.

If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500.00 of what the thief withdraws.

If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

VISA and MasterCard voluntarily have agreed to limit consumers’ liability for unauthorized use of their debit cards in most instances to $50.00 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card. However, the sooner you notify them, the better.

Be sure to write the financial institution by certified mail, return receipt requested, after calling them, so you can prove when they received the letter. Be sure and keep a copy of your letter for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. They must tell you the results of the investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

With regard to fraudulent checks, if an identity thief steals your checks or counterfeits checks from your existing bank account, then stop payment, close your account, and ask your bank to notify ChexSystems, Inc., or the check verification service with which it does business. If the account has been closed, you may call ChexSystems, Inc., yourself
at 1-800-428-9623. That way retailers can be notified not to accept these checks. You may be held responsible for the forgery if you fail to notify the bank in a timely manner that a check was lost or stolen.

To request that they notify retailers who use their databases not to accept your checks, call:
- TeleCheck at 1-800-710-9898 or 1-800-927-0188
- Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120.

To find out if the identity thief has been passing bad checks in your name, call:
- SCAN at 1-800-262-7771.

Other verification services are:
- CheckRite at 1-800-766-2748
- CrossCheck at 1-800-552-1900
- National Processing Co. (NPC) at 1-800-526-5380
- TeleCheck at 1-800-710-9898

If your checks are rejected by a merchant, it may be because an identity thief is using the Magnetic Information Character Recognition (MICR) code (the numbers at the bottom of checks), your driver’s license number, or another identification number. The merchant who rejects your check should give you its check verification company contact information so you can find out what information the thief is using. If you find that the thief is using your MICR code, ask your bank to close your checking account, and open a new one. If you discover that the thief is using your driver’s license number or some other identification number, work with your Department of Motor Vehicles, Division of Driver’s License, or other identification issuing agency to get new identification with new numbers. Once you have taken the appropriate steps, your checks should be accepted.

You may get additional help from the following agencies that oversee your bank:

For banks that are not members of the Federal Reserve System, and who insures deposits at banks and savings and loans:
- Federal Deposit Insurance Corporation (FDIC) @ www.fdic.gov

For state-chartered banks that are members of the Federal Reserve System:
- Federal Reserve System (FED) @ www.federalreserve.gov

Or, call 202-452-3693; or write: Division of Consumer and Community Affairs, Mail Stop 801, Federal Reserve Board, Washington, D. C. 20551. Federal Reserve Banks are located in Boston, New York, Philadelphia, Cleveland, Richmond, Atlanta, Chicago, St. Louis, Minneapolis, Kansas City, Dallas, and San Francisco.

For federal credit unions and many state credit unions:
- National Credit Union Administration (NCUA) @ www.ncua.gov
Or, call 703-518-6360; or write: Compliance Officer, National Credit Union Administration, 1775 Duke St., Alexandria, Va. 22314.

For national banks (if national appears in the name of the bank, or if the initials “N.A.” is in its name) the bank’s operations are overseen by:
Office of the Comptroller of the Currency (OCC) @ www.occ.treas.gov
Or, call toll-free: 800-613-6743 (business days from 9:00 am to 4:00 pm CST);
fax: 713-336-4301; or write: Customer Assistance Group, 1301 McKinney St., Ste. 3710, Houston, Tx. 77010.

For federal, and many state-chartered, thrift institutions, including savings banks and savings and loan institutions:
Office of Thrift Supervision (OTS) @ www.ots.treas.gov
Or, call: 202-906-6000; or write: Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552.

**Bankruptcy Fraud:** If you believe someone has filed for bankruptcy in your name, then write a letter to the U. S. Trustee (UST) in the region where the bankruptcy was filed, describing the problem and providing proof of your identity.

Following is a sample letter the U. S. Department of Justice suggested:

(Your name)
(Your address)
(Your daytime phone number)

(Date)

U. S. Trustee
(Local Office address)

Re: (Name of Debtor, Bankruptcy Number)

I have a complaint about a possible bankruptcy fraud. Here are the facts:

(Use one of the following)
1) I was turned down for credit on (date).
2) I obtained my credit report and found these errors on it:
3) I believe (or have evidence) that (name of person) stole my social security number (or name, or other identifying information) because:

(list all evidence and attach copies of all documents which show evidence of who used your identifying information).

Very truly yours,
(Your signature)

(Your printed name)

Enclosures

You may get copies of the documents filed, for a fee, by contacting the clerk’s office of the bankruptcy court. You may also contact them at their website www.usdoj.gov/ust. Be sure and keep copies of all your correspondence to and from the UST. You may also consider hiring an attorney to help you prove that the bankruptcy filing was fraudulent.

In addition, you may wish to file a report with the U. S. Attorney’s Office and/or the FBI in the city where the bankruptcy was filed.

**Correcting Fraudulent Information in Credit Report:** If you think you are a victim of identity theft, you need to contact the credit bureau, and the company that supplied them credit information, informing them that you are a victim of identity theft. Call the credit bureau and find out if they have a form you need to complete, and if so, have them send it to you. Complete either their report or the ID Theft Affidavit and mail it together with proof of your identity. Be sure to state that you did not make the debt or authorize it.

Please refer to our pamphlet entitled Florida Debtor’s Rights for more information.

**Credit Cards:** Procedures are spelled out for correcting errors on your credit card accounts under federal law, entitled the Fair Credit Billing Act.

First, call the credit card company or creditor to determine if they have a complaint form or if they would accept the ID Theft Affidavit, and find out what proof of identity they require.

After calling them, be sure to write the credit card company or creditor at the “billing inquiries” address, not the address for sending payment, indicating what information is incorrect on your statement. Be sure and send your letter and enclosures by certified mail, return receipt requested, so you know when they received the information. Be sure you contact them before the expiration of 60 days from first receiving the statement that contained the error. The credit card company or creditor must acknowledge receiving your complaint in writing within 30 days after receipt of your complaint. The credit card company or creditor must resolve the dispute within two billing cycles (but no more than 90 days) after receiving your letter.

**Criminal Violations:** If someone commits a crime using your identity, you will need to immediately contact the police department or sheriff’s office where the crime originated to file an identity theft report. Under Florida law, it is a crime to criminally use someone’s personal identification information.
If the arrest or crime was in a state or county other than where you live, then go to your local law enforcement office with sufficient information and copies of documents to prove your identity, and ask them to take a full set of your fingerprints, take a photograph of you, and for them to make copies of your driver’s license, passport, etc. Have them send the documentation to the state or county where the crime occurred and have the other state or county compare your fingerprints, etc., to those of the thief.

Eventually, law enforcement should recall any warrants issued against you. Ask them for a “clearance letter” or “certificate of release”. You will need to keep this document with you at all times in case you are wrongly arrested in the future.

You may wish to hire an attorney to help you clear your name. You may also need to clear your name in any court records.

**Debt Collectors:** Under the Fair Debt Collection Practices Act, debt collectors must follow certain guidelines and must treat a debtor fairly.

Within 30 days of the first contact by the debt collector or collection agency, you must advise them in writing, by certified mail, return receipt requested, so you can have a record of when they received your letter explaining that you are a victim of identity theft. Ask to complete their complaint form or ask if they will accept the ID Theft Affidavit. Forward the appropriate form to them, together with copies of your police report and proof of identity.

The debt collector or collection agency must tell the company that they are collecting for that you are a victim of identity theft. You must then contact the company to dispute the debt. If not, the company may send the debt to another debt collector or collection agency, report the bad debt to a credit bureau, or commence a lawsuit.

See our pamphlet entitled “Florida Debtor’s Rights” for more information.

**Driver’s License:** If your driver’s license is lost or stolen or someone has duplicated your license and using it for identification in cashing checks, etc., immediately contact the Florida Department of Motor Vehicles, Driver’s License Division, at your local office, which in DeSoto County, Florida, is the office of Kathryn J. Hill, Tax Collector, County Administration Building, 201 E. Oak St., Arcadia, Fl. 34266, or call 1-863-993-4861. After you report the loss or theft, then ask the person you speak to if they will contact the main office in Tallahassee, Florida, or if you need to contact them. You can get the Tallahassee telephone number from your local office.

Be sure to ask them to flag your license and file so that nobody else can get a license or any other identification document from them in your name.

**Investment Fraud:** Any complaints regarding investment fraud should be reported to the United States Securities and Exchange Commission (SEC). You may contact them at [www.sec.gov/complaint.shtml](http://www.sec.gov/complaint.shtml) You may also write them at: SEC Office of Investor
Education and Assistance, 450 Fifth Street, NW, Washington, DC 20549-0213, or call them at 202-942-7040.

If someone has tampered with your securities or brokerage account, be sure to report it to your securities broker or the account manager, as well as the Securities and Exchange Commission.

**Long Distance:** If an identity thief is billing long distance calls to your cell phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs. If you’re having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the following agency:

Federal Communications Commission FCC @ [www.fcc.gov](http://www.fcc.gov)
You may also call: 1-888-CALL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, Room 5A863, Washington, DC 20554.

The FCC also regulates interstate and international communications by radio, television, wire, satellite, and cable.

**Mail Theft:** The U. S. Postal Inspection Service (USPIS) is the law enforcement arm of the U. S. Postal Service, and they investigate cases of identity theft. If an identity thief has stolen your mail to get new credit cards or bank or credit card statements, pre-screened credit offers, or tax information, or has falsified change-of-address forms or obtained you personal information through a fraud conducted by mail, report it to your local postal inspector. You can obtain their phone number from your local post office. You may also contact them @ [www.usps.gov/websites/dep/inspect](http://www.usps.gov/websites/dep/inspect)

**Military:** If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When you place an active duty alert, you’ll be removed from the credit reporting companies’ marketing list for pre-screened credit card offers for two years unless you ask to go back on the list before then. The process for getting and removing an alert are the same as that for an initial alert described earlier in this pamphlet.

**Passport Fraud:** If you’ve lost your passport, or believe it was stolen or is being used fraudulently, contact the United States Department of State (USDS) @ [www.travel.state.gov/passport/passport_1738.html](http://www.travel.state.gov/passport/passport_1738.html) You may also contact them at their local field office. You may check with the Clerk of the Court at the Courthouse to get their local field office address.
**Phone Fraud:** If an identity thief has established local phone service in your name, immediately contact your local phone service provider to cancel the incorrect local phone service. If you’re having trouble getting fraudulent phone charges removed from your name or getting an unauthorized account closed, contact the Florida Public Service Commission @ [www.psc.state.fl.us](http://www.psc.state.fl.us) or call: 1-800-342-3552 for Consumer Affairs.

**Scholarships:** If you become a victim of identity theft involving federal education funds or suspect that your student information may have been stolen, contact: U. S. Department of Education, Office of Inspector General @ [oig.hotline@ed.gov](mailto:oig.hotline@ed.gov) or you may call: 1-800-647-8733.

**Social Security Number Misuse:** If your Social Security Number is lost or stolen, it may be used by someone to file a tax return in order to receive a refund. If they file the tax return first, the IRS may believe that you already filed and received your refund. It may also be used by an undocumented worker to get a job. That person’s employer would report income earned to IRS making it appear that you did not report all of your income on your tax return.

If you receive a notice from IRS that leads you to believe someone may have used your Social Security Number fraudulently, please notify IRS immediately by responding to the name and number printed on the notice or letter, in writing, at the address given in the notice. You may also call them at 1-800-829-1040.

You may consider obtaining a new Social Security Number. However, that may not resolve your identity theft problems, and may create new problems. A new number does not ensure a new credit record because credit bureaus may combine the credit records from your old number and those with your new number.

To report your Social Security card lost or stolen, you may contact Social Security Administration @ [www.ssa.gov](http://www.ssa.gov) or go to your nearest office. You can replace your Social Security card no more than 3 times in a year and only 10 times in a lifetime.

If you decide to apply for a new Social Security Number or obtain a replacement card there are new rules that apply. You will need to prove your U. S. citizenship or immigration status, your age and your identity. Under the new law, only certain documents can be accepted as proof of U. S. Citizenship. These include your U. S. birth certificate, a U. S. Passport, a Certificate of Naturalization or a Certificate of Citizenship.

Also under the new law, only certain documents can be accepted as proof of identity. If you are a U. S. Citizen, then Social Security must see your U. S. driver’s license, a State-issued nondriver identity card, or a U. S. Passport.

If you are not a U. S. citizen, they must see your current U. S. immigration documents. Acceptable documents from the Department of Homeland Security include your Form I-551, your I-94 with your unexpired foreign passport, or work permit card (I-766 or I-688B).
You will need to take all these documents to your nearest Social Security Administration office.

If you have specific information of a Social Security Number misuse that involves the buying or selling of Social Security cards, that may be related to terrorist activity, or is designed to obtain Social Security benefits, contact the SSA Office of the Inspector General. You may file a complaint online at www.socialsecurity.gov/oig or call toll-free at 1-800-269-0271 or fax 1-410-597-0118 or write: SSA Fraud Hotline, P. O. Box 17768, Baltimore, MD 21235.

You also may call SSA toll-free 1-800-772-1213 to verify the accuracy of the earnings reported on your Social Security Number or request a copy of your Social Security Statement. Follow up in writing.

**Student Loans:** If someone opens a fraudulent loan in your name, contact the school or program that opened the student loan to close it. At the same time, report the fraudulent loan to U. S. Department of Education. Call the Inspector General’s Hotline toll-free at 1-800-MIS-USED; visit www.ed.gov/about/offices/list/oig/hotline.html?src=rt or write: Office of Inspector General, U. S. Department of Education, 40 Maryland Avenue, SW, Washington, DC 20202-1510.

**Tax Fraud:** The IRS is responsible for administering and enforcing tax laws. Identity theft may occur as it relates directly to your tax records. You may contact IRS on the internet at www.irs.gov and type in the IRS key word “identity theft” for more information.

If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service website at www.irs.gov/advocate/ or call toll-free: 1-877-777-4778.

**8. PRECAUTIONS TO TAKE TO AVOID BECOMING A VICTIM.**

To reduce or minimize the risk of becoming a victim of identity theft, there are some basic steps you can take. For starters, just remember the word “SCAM”:

S  Be *Stingy* about giving out your personal information to others unless you have a reason to trust them.

C   Check your financial information regularly, and look for what should be there and what shouldn’t.

A   Ask periodically for a copy of your credit report.
M Maintain careful records of your banking and financial accounts.

Additional precautions against identity theft are:

- Freeze your credit, if available. With a credit freeze, no one can open any form of credit in your name.
- Request your own credit report each year and check for inaccuracies and new lines of credit that you did not request.
- Minimize the use of mail for sending or receiving financial documents, checks, and have your name removed from junk mail lists. Install a locking mail box at your residence if you do not have a post office box.
- Check your bank accounts each week online or at an ATM.
- Use reliable ATM’s at reputable sites only. Watch your surroundings for anything suspicious. If the interior of a bank is closed but an indoor ATM is still accessible with a card, refuse helping any stranger to enter. Look for suspicious attachments to any ATM that may steal information. If in doubt, do not use the ATM but report the problem.
- Watch your surroundings when entering sensitive codes of information at an ATM or on a telephone keypad. Enter sensitive things with touch-tone but not voice entry. Hide what you type on a keypad from others.
- Do not use a wireless phone or cellular phones to talk about sensitive information. Use a wired phone connected to the ground or encrypted Internet access.
- Shred credit-card receipts, used (processed) checks, junk mail and other such documents, as they may contain private information.
- Never give out personal information in response to telemarketers and delete all e-mails that claim to be from your bank (or other financial provider) and ask you to “log in” using a hyperlink embedded in the e-mail message. If in doubt as to the legitimacy of such requests, use a telephone to call marketers or financial providers back (rather than directly responding to the telemarketer or company that called or emailed you).
- When shopping online, make sure the company is reputable and displays an approved security symbol. Also, make sure you log out of the site when finished. Also, before ordering by mail or phone, check the firm’s reputation with your local Better Business Bureau or with Florida’s consumer hotline at: 1-800-435-7352.
- Watch your surroundings when using a credit card at any checkout counters or any similar places as some identity thieves use cell phones with cameras to steal others’ credit card numbers and expiration dates. (This is why certain stores now prohibit taking pictures and videos without consent.)
- If you are a target, keep copies of police reports and records of who you talked to and when, so that you can back up the claim of theft and fraud. Individuals who consider themselves at higher risk of identity theft should consider purchasing fee-based credit monitoring services, which will notify you of any new accounts or credit inquiries made on your behalf.
Limit the amount of personal information you publish on the web. Small fragments here and there may be enough for someone to impersonate you in many ways. Be especially careful with information used as security keywords for banks, e.g. mother’s maiden name and give your bank a different word (a password) instead of the real maiden name. Place passwords on your credit cards, bank and phone accounts.

Don’t divulge personal information such as date of birth to organizations that have no need of it.

Do not routinely carry your Social Security card unless absolutely needed. Don’t give out the number unless it is absolutely necessary or legally required (employers, landlords, etc.)

Do not allow anyone to copy your identification documents except for law enforcement or to prove identity in clearing up an identity theft matter. If commercial organizations require you to submit a copy as a condition of doing business either don’t do business with them, or retrieve the copy when your business ends (and a written statement that they have not taken further copies should be obtained).

If someone calls you claiming to be from a financial institution you do business with asking for personal information, do not give it to them. Ask them why they want the information, hang up, and then call the institution (using contact information from a source other than the caller).

Don’t order checks preprinted with your driver’s license or Social Security number. If you can keep your address off them, do so. When ordering new checks, pick them up from the bank instead of having them mailed to your home.

Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done at your home.

Ask about information security procedures in your workplace or at businesses, doctor’s offices or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

Treat your mail and trash carefully. Invest in a shredder. A crosscut paper shredder works best.

Keep your purse or wallet in a safe place at work; do the same with copies of forms that have your sensitive personal information.

Opt out on pre-approved credit offers and the “convenience checks” that often accompany them to get a credit card quickly. According to the postmaster general, 30 percent of convenience checks get used fraudulently. If you want fewer pre-approved credit offers in your mailbox, you can call 1-800-5-OPT-OUT and ask them to remove your name and address from the mailing lists. You may also write to: DMA Mail Preference Service, P. O. Box 9008, Farmingdale, NY 11735-9008. To avoid unwanted telephone sales calls from many national marketers,
send your name, address and telephone number to DMA Telephone Preference Service, P. O. Box 9014, Farmingdale, N.Y 11735-9014. Florida law also authorizes consumers to be placed on a special “no sales solicitation calls” listing by paying $10 (with a $5 per year renewal fee) to Florida’s Department of Agriculture and Consumer Services. For details, or if you believe you were defrauded, contact Florida’s Consumer hotline at 1-800-435-7352.

✓ Do not have conversations about your bank accounts or credit in public.
✓ When using the internet, keep your computer, and the personal information it stores, safe. Some of the various ways are: install virus protection software and keep it updated regularly; do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don’t know; use a firewall program; use a secure browser – software that encrypts or scrambles information you send over the internet; try not to store financial information on you laptop unless absolutely necessary; before you dispose of a computer, delete all personal information it stored (reformatting your hard drive may not be enough…use a “wipe” utility program to overwrite the entire hard drive); and look for website privacy policies…if you don’t see one or can’t understand it, consider doing business elsewhere).
✓ Be careful selecting your tax preparer if you do not prepare your own return. They have access to all your personal financial records.

9. STAYING ALERT.

Once resolved, most cases of identity theft stay resolved. However, some victims have recurring problems. To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully. You may want to review your credit reports once every three months in the first year of the theft, and once a year thereafter. Be sure to stay alert for other signs of identity theft, such as:

✓ Failing to receive bills or other mail.
✓ Receiving credit cards you didn’t apply for.
✓ Being denied credit or offered a high interest when not warranted.
✓ Getting calls or letters from debt collectors about merchandise or services you didn’t buy.

To order your free annual report from one or all of the national consumer reporting companies, visit www.annualcreditreport.com or call toll-free 1-877-322-8228, or obtain the Annual Credit Report Request Form from www.ftc.gov/bcp/conline/include/requestformfinal.pdf and mail it to Annual Credit Report Request Service, P. O. Box 105281, Atlanta, Ga. 30348-5281. Do not contact the three nationwide consumer reporting companies individually. They provide free annual credit reports only through www.annualcreditreport.com, 1-877-322-8228, and Annual Credit Report Request Service, P. O. Box 105281, Atlanta, Ga. 30348-5281.
Under federal law, you’re entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company.

The information for the foregoing pamphlet was obtained from the following websites:

www.ftc.gov
www.ssa.gov
www.irs.gov
www.ed.gov
www.usps.gov
www.usdoj.gov
www.myfloridalegal.com
www.flsenate.gov/Laws/Statutes/
www.wikipedia.org/wiki/identity_theft
http://money.cnn.com
www.bbb.org

THIS PACKET PROVIDED FOR YOUR USE BY:

HONORABLE DON T. HALL
COUNTY JUDGE
DESOТО COUNTY, FLORIDA
115 EAST OAK STREET, SUITE 201
ARCADIA, FLORIDA 34266