A citizens guide to

IDENTITY THEFT

made available by the

DAYTONA BEACH POLICE DEPARTMENT

IDENTITY THEFT

"Identity theft" is the term used to describe a theft in which the thief uses your name, social security number, credit card number, or other identifying information without your permission to commit fraud or other crimes.

In most cases a thief will not actually assume your identity, he or she will merely "borrow" your credit. It's common for thieves to run up enormous bills in your name after gaining access to one of your existing accounts, or by opening new accounts in your name. Often the victim of an identity theft is unaware of what has occurred until they apply for new credit, or are denied for credit themselves.

In the past identity theft has been difficult to report, difficult to investigate and difficult for victims to recover from. The following information has been gathered from several very good resources and is presented here as a single reference point. This information will be helpful to those looking to help protect themselves and / or those who have already been the victim of an identity theft.

How Does Identity Theft Occur?

Identity thieves use several different methods to obtain your personal information in order to steal from you. Many of these methods are simple; some are very clever. Listing a "how-to" guide describing exactly how this can be done would not be in the best interest of crime prevention. There are, however, a few general methods that you should be aware of, so you can be on alert for them:

- **Stealing Mail:** Your unlocked mailbox holds a wealth of information. Incoming mail often includes pre-approved credit card offers, and outgoing mail often includes checks you've sent out as payments.

- **Dumpster Diving:** If you fail to shred your pre-approved credit card offers, bank statements, and other papers that contain your personal information before you throw them away, thieves can easily pick them out of the trash and take that information.

- **Fraudulently Obtaining PIN Numbers:** Thieves have been known to look over people's shoulders as they enter their PIN's. They have even been known to install fake covers over existing ATM machines that appear to be part of the machine. This device will record the information from your card (Including the PIN you enter). You'll just get a screen telling you that the ATM is out of money (Which does legitimately occur), and the thief can return later to recover his device, which now has your account number and PIN recorded in it.

- **The Internet:** Thieves will often mail out unsolicited e-mails that request detailed information about the recipients. This information often includes credit card numbers and personal identification that should not be shared. Most Internet users won't respond to this, and many will report the activity to their Internet service provider, but several unsuspecting individuals will responded to the e-mail and simply give away their most personal information.

- **Skimming:** There are small handheld devices (Skimmers) that can be used to scan a credit card and record its information. Many of these devices run on batteries, fit in your pocket, and can hold information from hundreds of cards. Identity thieves will pay people (For example waiters and waitresses) to fill these devices with credit card numbers. The information is then downloaded to a household computer and / or recorded onto blank cards.

- **Businesses:** Several businesses keep databases of employee information and are often the target of computer hackers. Other businesses enter your information into their computers and then throw away the printed information without shredding it.

Identity Theft Prevention Tips

There are several things you can do to minimize the risk of becoming the victim of an identity theft. The first step in protecting yourself would be realizing that identity thieves use several different methods to obtain and exploit your personal information. A few of the methods are described above, but there are many others that involve the trail of personal information you leave behind during your daily activities. By making slight changes in your daily routine you can help prevent a criminal from obtaining that information.

TIPS:

- Check your credit report at least once a year and closely review it for inaccuracies.

- Carefully review your monthly credit card and bank statements the day you receive them. Immediately report any discrepancies (Waiting more than 2 days to report a discrepancy could raise the amount you can be held responsible for from 50. to 500. dollars, or more).

- Be more defensive with your personal information. Ask salespeople and others if information such as your social security number or driver's license number is absolutely necessary. Ask anyone who does require this information what their privacy policy is, and if you can ask that they don't share that information with anyone else.

- Never give your personal information (Social Security Number, Date of Birth, Bank Account Numbers, Credit Card Numbers, etc.) to an unsolicited caller, even if they state they represent your bank, or even if they ask you to punch it in by number.

- Limit the number of ID's and Credit Cards you carry with you to what you'll actually need.

- Consider closing all unused credit card or bank accounts in your name (Consider keeping the credit card you've had the longest, or the one with the highest balance so that this does not hurt your credit score).

- Before throwing them away be sure to shred your bank statements, credit card receipts, pre-approved credit card applications, and any other items listing your personal or financial information.

- Do not carry your Social Security card (or any card with your social security number on it) in your wallet or purse. You should keep such a card that has this information (Like your insurance card) in a secure place, and only carry it with you when it's needed.

- Protect your PIN number. Make sure no one can see the keypad as you're entering your PIN number at an ATM, or Department store register.

- Never leave receipts at ATM's, Bank Counters, Restaurants, Etc.

- If your ever presented with a receipt that has your credit card number printed on it, cross it out when you sign the receipt. The retailer has already captured this number electronically and does not need the printed version, which they may not shred before throwing away.

- Don't leave outgoing mail in your residential mailbox for pick up – Deposit it in a secure Post Office Collection Box or at the Post Office itself.

- Pay attention to your billing cycles. If a bill or statement does not arrive on time it may mean that someone has changed your billing address.

- Consider a locking mailbox for your residence to protect incoming mail.

- Beware of promotional solicitations through the mail or by the telephone that offer you instant prizes or awards and seek to obtain your personal information or credit card numbers.

- When making an online purchase look in the lower right hand corner of your browser window. If you see the icon of a lock, it means you're dealing with a secure site. That pages web address should also have "https" in its address. If you don't see these, you might be safer using another merchant.

- Use only one credit card for online purchases, that way it will be easier to spot suspicious activity on your bill.

- If you are suspicious of credit card "skimming", or how a business might handle your credit card information, pay with cash.

- Collect and keep a list of contact numbers from your monthly statements in a secure place. This list will be helpful when reporting your credit card / bank cards lost or stolen.

- Remove your name from the mailing lists for pre-approved credit lines by calling **1-888-567-8688.**

- Remove your name, phone number, and home address from marketing list by contacting the Direct Marketing Association. This will not prevent your name from being placed on all marketing lists, but it removes your information from many of them.

  DMA Mail Preference Service
  P.O. Box 9008
  Farmingdale, NY 11735-9008

  DMA Telephone Preference Service
  P.O. Box 9014
  Farmingdale, NY 11735-9014

  Both of the above are available online at: www.the-dma.org.

  There is also a web site where you can go to remove your e-mail address from many national marketers e-mail list. It is www.e-mps.org.

If you become the victim of an Identity Theft

The most common types of identity theft involve someone else using your personal information to either steal from your existing credit accounts, or fraudulently obtaining new credit in your name. These crimes are usually discovered when the victim receives his or her bank statement in the mail, or when the victim is denied credit based upon the fraudulent accounts becoming delinquent.
As soon as you realize that your information has been misused in this manner, there are five steps you should take:

1). Report the incident to the fraud department of the three major credit bureaus.

- Ask the credit bureaus to place a "fraud alert" on your credit report.

- Order copies of your credit reports so you can review them to see if any additional fraudulent accounts have been opened in your name or if any unauthorized charges have been made to other accounts.
  The Fair Credit Reporting Act of 2003 requires each of the three credit bureaus to supply you (Upon your request) with a free copy of your credit history (1 each year, 2 if you have been the reported victim of identity theft).
  To do this either visit www.annualcreditreport.com or call 1-877-322-8228. This is a free service and does not require you signing up for a pay service that needs to be canceled at a later date like many links that are sent out via e-mail.

- Do not contact the three nationwide consumer-reporting companies individually to ask for a free copy of your credit report. They are providing free annual credit reports through the link above.

  If you do need to contact the three nationwide consumer-reporting companies directly for any other reason their contact information is as follows:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
To report fraud: 1-800-525-6285
TDD: 800-255-0056
www.equifax.com

TransUnion
Fraud Victim Assistance
P.O. Box 6790
Fullerton, CA 92634-6790
Email: fvad@transunion.com
To report fraud: 1-800-680-7289
TDD: 877-553-7803
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
To report fraud: 1-888-EXPERIAN (397-3742)
TDD: 800-972-0322
www.experian.com

2). Contact the fraud department of each of your creditors.

- Gather contact information for each of your credit accounts (credit cards, utilities, cable bills, etc.) and call the fraud department for each creditor.

- Report the incident to the fraud department of each of your creditor's, even if your account at their institution has not been tampered with. Close the accounts that you believe have been compromised. Ask the credit bureaus to place an "alert" on any accounts that remain open.

- Immediately follow up your phone call with a letter and any necessary documentation (Including the police report) to support your claim. The Federal Trade Commission provides an 'Identity Theft Affidavit' that may make this easier (The affidavit is a standardized form used to report *new* accounts fraudulently opened in your name - See #5, below). Check with the company to see if they accept this form. If not, request that they send you their fraud dispute form.

3). Contact your bank or financial institution.

- **This needs to be done as soon as possible.** If the theft involves any type of electronic fund transfers (ATM cards, Debit Cards, or other electronic withdrawals from your bank account) your liability is determined by how long it takes you to report the crime. The Electronic Fund Transfer Act limits the amount you can be held responsible for to $50.00, **if** you report your loss / theft within two business days. If you report your loss after 2 days, but within 60 days of a statement showing the unauthorized electronic fund transfer, you can be liable for up to $500.00. If you wait more than 60 days you can lose all the money that was taken from your account.

- If your checks have been stolen, or if you believe they have been used, contact your bank or credit union and stop payment right away.

  Contact the major check verification companies and request they notify retailers who use their databases not to accept your checks:

  TeleCheck 1-800-710-9898 or 927-0188
  Cetergy, Inc 1-800-437-5120
  International Check Services 1-800-631-9656

- Call SCAN at 1-800-262-7771 to learn if bad checks have been passed in your name.

- If you suspect your accounts have been compromised, cancel your checking and savings accounts and obtain new account numbers.

4). Report the incident to law enforcement.

- Contact your local Police Department or Sheriffs Office to file a report. Under Florida Statute 817.568, the report may be filed in the location in which the offense occurred, or, the city or county in which you reside.

- When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.

- Ask that your police report be flagged in a way so as only you can get a copy of it (Not available to the public).

- Keep your report number handy, and obtain a copy of the report once it is available. Most creditors will request to see the report before they will remove the fraudulent debts from your account.

5). Report the incident to the Federal Trade Commission (FTC).

- All victims of identity theft should file a complaint with the Federal Trade Commission (FTC). The FTC maintains a database of identity theft cases to assist law enforcement agencies investigating this crime. To file a complaint with the FTC call 1-877-438-4338; TDD: (202) 326-2502. or go to https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03 .

- The FTC has also developed an 'ID Theft Affidavit' to help victims of identity theft in reporting information to many different creditors using just one standard form. The use of this affidavit is optional, and it is only used when the thief has opened ***new*** accounts and obtained ***new*** credit in your name.
  For a copy of the ID Theft Affidavit visit:
  www.ftc.gov/bcp/edu/microsites/idtheft/

  Remember this affidavit is to be sent to your creditors, do not send it to the FTC or any other government agency expecting them to disperse this information.

There are also several other means by which criminals can misuse your personal information, some of these effect your:

Mail

If information obtained from your stolen mail has been used by an identity thief to obtain new credit, or commit a fraud using your name the United States Postal Inspection Service will also investigate the crime. Incidents should be reported to the US Postal Inspection Service office nearest you.
The office serving the Daytona Beach area is:
Postal Inspection Service
3400 Lakeside Dr. FL 6
Miramar, FL 33027-3242
Phone: (954) 436-7200
Fax: (954) 436-7282
For other offices visit www.usps.com .

Phone

If an identity thief has established new phone service in your name, or is making unauthorized calls that seem to come from – and are billed to your account (Cellular or landline) you should contact your service provider as soon as possible to have the accounts closed.
If you have difficulties getting fraudulent phone charges removed from your account contact the Florida Public Service Commission at www.floridapsc.com.

Social Security Number

The Social Security Administration (SAA) can verify the accuracy of the earnings reported on your social security number. To check for inaccuracies or fraud, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) by calling the Social Security Administration at 1-800-772-1213, or visiting www.ssa.gov .
If you have confirmed that your Social Security Number has been stolen or misused contact the SSA Fraud Hotline at 1-800-269-0271 or by visiting www.ssa.gov/oig/guidelin.htm.

Criminal History

In some instances of identity theft, a 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 see if any arrest records have been falsely associated with you as a result of someone else using your identity. If a check of your fingerprints determines that you are an identity theft victim, FDLE will work with local law-enforcement agencies to attempt to clear fraudulent data from your criminal history and provide you with a Compromised Identity Certificate. For more information, contact FDLE's Quality Control Section at (850) 410-8880, or visit www.fdle.state.fl.us/CompID/ .

Driver's License

It shouldn't happen, but it's possible that someone other than you could give your name in a traffic stop and be issued a citation under your driver's license number. If you ever receive a notice claiming that you have not paid a citation (Especially one you don't remember receiving), contact your local Department of Highway Safety and Motor Vehicles (DHSMV) as soon as possible.
If you have been the victim of an identity theft you may request that the fraud section of the DHSMV place a flag on your driver's license alerting police in the future to double-check your identity when your name / driver's license number is checked.
The DHSMV web site is http://www.hsmv.state.fl.us.
Also under Florida state law, motor vehicle and driver license records are subject to public disclosure. The Driver Privacy Protection Act (DPPA) allows you to keep your personal information private, by limiting who has access to the information. To complete a 'Request to Withhold Disclosure of Personal Information' form online go to www.hsmv.state.fl.us/html/disclosure.pdf .

Court Records
If you believe there is an official court record (Often available to the public) that lists your Social Security Number, Bank Account Number, Credit Card number, etc. you can contact your local County Court Clerk and ask that they redact / remove that information.
The Volusia County Clerk of the Court is:

DIANE M. MATOUSEK
Address 101 N. Alabama Ave., Deland, FL 32724
Telephone (386) 736-5915 or (386) 736-5915
Fax (386) 822-5711
SUNCOM 377-5710

A listing of all Florida's County Clerks can be found at www.flclerks.com .

Passport
If your passport is lost or stolen, or if you believe your passport is being used fraudulently contact the Department of State at (202) 955-0430 (24Hr.s a day). The Department of State Web Site is http://www.state.gov.

Frequently Asked Questions

Q: My credit card was used to make purchases in Florida cities far away from where I live (Or online, or another state). Do I need to call the police in those areas?
A: No, according to Florida law (FSS 817.568) the report may be filed in the location in which the offense occurred, **or**, the city or county in which you reside. This law was created to ensure that victims are provided an opportunity to report I.D. Theft as soon as possible.

Q: Am I responsible for the bills identity thieves run up in my name?
A: Federal credit fraud law protects you here. Credit card and other companies that wrongly extend credit in your name must obtain the money from the identity thief, or suffer the losses. They are still allowed to ask you to pay them a $50.00 fee, but most creditors realize their loss came from their business practices and usually won't ask you for that money. This does not, however, apply to ATM Cards, Debit Cards, or Electronic fund transfers that withdrawal funds from your existing bank account. With regards to these accounts the amount you are held responsible for depends on how long you wait to report the theft / loss. The Electronic Fund Transfer Act limits the amount you can be held responsible for to $50.00, if you report your loss / theft within two business days. If you report your loss after 2 days, but within 60 days of a statement showing the unauthorized electronic fund transfer, you can be liable for up to $500.00. If you wait more than 60 days you can lose all the money that was taken from your account.

Q: I've heard that there are Credit Monitoring Services that can help protect me from Identity theft. Do they work?

A: These services check your credit on a regular basis (This could be quarterly, or otherwise depending on how much you are willing to pay) and notify you of any credit that has been applied for, or issued, under your name. Some of these services are quite expensive and experts debate how helpful they really are.

Q: What is Credit Freezing?

A: Some states (California and Texas) have passed laws allowing their resident's to freeze their credit so that identity thieves can't open new accounts in their names. Once a persons credit is "frozen" it requires a personal identification number (that only the consumer knows) to unfreeze the account and enable new credit to be granted.

RESOURCES:

Daytona Beach Police Department
http://www.DBPD.us
U.S. Dept of Justice
http://www.justice.gov/
U.S. Dept of State
http://www.state.gov
Federal Trade Commission
www.ftc.gov/
Florida Dept of Law Enforcement
www.fdle.state.fl.us/
Identity Theft Resource Center
www.idtheftcenter.com/
Florida Department of Highway Safety and Motor vehicles
http://www.hsmv.state.fl.us
Social Security Administration
www.ssa.gov

From our Legal Department:

The above information is being provided as a public service and is not intended as legal or financial advice. The information herein was obtained from the several Resources listed above. The D.B.P.D. does not guarantee the accuracy of the contents.

The information contained herein was current and up to date at the time of publishing. Because laws are updated often, and sometimes differ from state to state, it is recommended that you contact your local Police Department if you have any questions. With the exception of the Daytona Beach Police Department web site, the web sites above are maintained by their respective agencies.

DBPD/JT