Justice Starts Here

Identity Theft Prevention Program

Provided by
KATHERINE FERNANDEZ RUNDLE
State Attorney
Eleventh Judicial Circuit
Miami-Dade County

Community Outreach Division
305-547-0724

Provided by
KATHERINE FERNANDEZ RUNDLE
State Attorney
Eleventh Judicial Circuit
Miami-Dade County

IDENTITY THEFT PREVENTION PROGRAM

Identity theft is when someone takes your ***personal information*** to obtain monetary loans, obtain credit or other types of monetary benefits. Identity theft also occurs when someone uses your name or personal identifiers to evade responsibility for other criminal offenses, or to harass others.

HOW IDENTITY THEFT OCCURS

Skilled identity thieves use a variety of methods to gain access to your personal information. For example:

- They rummage through your trash, or the trash of businesses or dumps in a practice known as "dumpster diving."
- They steal credit and debit card numbers as your card is processed by using a special information storage device in a practice known as "skimming."
- They steal wallets and purses containing identification and credit and bank cards.
- They steal incoming or outgoing mail, including bank and credit card statements, pre-approved credit offers, new checks, tax information, or checks made payable for balances due on existing accounts.
- They scam information from you by posing as a legitimate business person or government official.

The following are examples of ***personal information*** you shouldn't give out:

- Date of birth
- Social security number
- Driver's license number
- Passport number
- Names of companies where you have credit
- Banks where you have your bank accounts
- Mother's maiden name
- Account passwords
- Other personal data

STEPS TO HELP PREVENT IDENTITY THEFT

1. **Do not give any type of personal information to unknown individuals, whether over the phone, in writing or on the Internet.**
2. **Protect your PIN (Personal Identification Number)** numbers and passwords that allow access to your accounts.
    a. Change pre-set PINs and passwords so that they are only known to you.
    b. Do not give your secret PIN numbers to anyone.
    c. Do not write these numbers on the credit or debit cards.
    d. Do not write these numbers on post-it notes and leave them in areas where they might be found, such as under keyboards, or posted to computer monitors.

e. Do not use PINs that can be easily guessed, such as your address, birth date or the last 4 digits of your Social Security Number (SSN) – Simply put, do not use any identifiers that could be found on your credit report as your PIN – doing so may allow an identity thief to compromise multiple accounts by simply ordering your credit report.
f. Try to avoid using the same PIN for multiple accounts.
g. Change PIN numbers on all your accounts more than once a year – if the new PINs are too difficult to remember, avoid using a list that if found, would compromise your accounts. Instead, try using hints that would serve as reminders to you and only you for the PIN for each account.

3. **Do not leave outgoing mail in your residential mailbox** for the postman to pick it up – deliver your outgoing mail instead to an official postal drop box, preferably one located at a U.S. Post Office. **Pick up the delivered mail as soon as possible after the postman leaves it in your mailbox**. Similarly, when leaving for vacation, fill out a hold request with your local U.S. Post Office. **Consider buying a locking mailbox** that allows mail to be deposited by your local letter carrier, but not removed without a key.
4. **Be aware of the dates when you are expecting checks in the mail** (criminals know more or less when government checks arrive). If possible, request direct deposit instead of a check.
5. **Determine whether you have been receiving your mail at scheduled intervals.**
   a. If several days pass by without receiving any mail, call or go to your corresponding post office and find out why you have not received the mail. Identity thieves often falsify a post office change-of-address form to have legitimate mail, including bank and credit card statements, re-routed so account information goes to another address where they can access those items, or will order the mail to be held at the post office so the thieves can retrieve it using fake identification with your name and address but their picture.
   b. If an identity thief has stolen your mail for access to new credit cards, bank and credit card statements, pre-approved credit offers and tax information or they have falsified change-of-address forms, you should report the crime to your local postal inspector. You may contact the U.S. Postal Inspection Service online at: http://www.usps.com/websites/depart/inspect/.
   c. If an identity thief has changed the billing address on an existing credit card account, you should close the account immediately. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. That password should be different than the one used for the previously compromised account.

6. **Be aware of identity theft scams that appear to be sweepstakes, raffles or surveys**.
7. **Limit the identification information and the number of credit and debit cards that you carry** to what you'll actually need for the day or period of travel.
8. **Limit the amount of information containing your personal identifiers that may be publicly available**: For example, Florida State law subjects your motor vehicle and driver's license records to public disclosure - you may be entitled to limit the release of personal information contained in your Florida motor vehicle and driver's license records. You may contact the Florida Department of Highway Safety and Motor Vehicles and request a limitation on the release of your data at http://www.hsmv.state.fl.us/html/withhold.pdf. For further information, go to http://www.hsmv.state.fl.us/ddl/DPPAInfo.html.

9. To thwart an identity thief who may pick through your trash or recycling bins, **tear or shred all documents containing personal identifiers prior to discarding**, such as charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements, and expired charge cards.
10. **Be aware of your surroundings when using your ATM card, debit card or credit card**. If a store or restaurant attendant has to swipe your card, watch to see if it is swiped more than one time or on more than one terminal. If you are using the card at an automated teller machine, cover the keypad with one hand while entering your PIN with the other to avoid "shoulder surfers." Avoid using ATMs that seem unusual, altered, or not maintained by a reputable bank.
11. **Make a photocopy of the front and back of all of your ATM cards, debit cards or credit cards and keep that copy in a safe place**. This will save precious time if your wallet or purse containing your credit cards is lost or stolen.
12. **Purchase and install security software such as firewalls, anti-virus and anti-spyware programs** on your personal computer and electronic devices. Update these programs when new versions are made available.
13. **Ignore suspicious emails or unsolicited emails** ("spam"), particularly those that appear to be from banks, credit card companies, financial institutions and internet service providers. Legitimate businesses, particularly banks, do not contact customers or account holders via unsolicited emails to request personal identifiers and account information. Computer users should attempt to completely ignore these types of emails, which are commonly referred to as "phishing," because simply opening them could unleash embedded programs ("spyware") that could be stored on your computer and actually report passwords or keystrokes over the internet to offenders responsible for the email. If you mistakenly open the email, you should **avoid clicking on any links contained within the suspicious email**. Forward any suspicious emails that are "phishing" for information to spam@uce.gov and check with the legitimate company that the email is purportedly from, regardless of whether you were induced to provide your information. Most banks, credit card companies and financial institutions have information on their websites that tell consumers where to report phishing emails. However, do not click on any of the content within the fraudulent email in order to go to the company website – instead, simply close the email and use your web browser and any well known search engine to find the correct webpage, or utilize the phone book to find the legitimate company's contact information. For more information, visit http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm and also http://onguardonline.gov/stopthinkclick.html.
14. **Be careful when typing web addresses and verify the correct spelling of a web address before hitting the browser's send button**. In anticipation of misspelled addresses, offenders have set up "spoofed" web sites with the misspelled web address but designed to look like the legitimate site, and poised to accept personal information, like credit card account numbers and passwords, entered by users who mistakenly believe they are at the legitimate page.

15. **Order your credit report from each credit reporting agency once a year in order to review it** and verify information. Since June 1, 2005, Florida residents are entitled to order a free annual credit report from each of the major credit reporting agencies in accordance with FACTA (Fair and Accurate Credit Transactions Act). **To order your free reports, you can call 877-322-8228 or go to** www.annualcreditreport.com. Because federal law requires free reports once yearly, and there are three major credit reporting agencies, you may order three free reports a year. Thus, we recommend that you order one every four months on a rotating basis from each of the three agencies. Review those reports carefully and contact any listed creditors that have reported erroneous information or creditors for accounts that appear suspicious or fraudulent to you.

IF YOUR IDENTITY HAS BEEN COMPROMISED, TAKE THE FOLLOWING STEPS

Unfortunately, victims bear much of the burden in resolving the problems associated with identity theft. If victimized, you must act quickly and assertively to minimize the damage. In dealing with the authorities and financial institutions, ***keep a log*** of all conversations, including dates, names, and phone numbers. Confirm conversations in writing. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents, including receipts for expenditures related to minimizing the damage and repairing your credit. Keep copies of all documents sent to and from creditors. Create a filing system to organize the files to ensure quick and efficient access when communicating with creditors and law enforcement. The following chart may be helpful for documenting whom you spoke with, when, and for organizing phone numbers: http://www.ftc.gov/bcp/conline/pubs/credit/idtheftform.pdf

1. **File a police report** in the community where the crime took place (if you don't know where the crime occurred, call your local police). Make sure the police report lists the fraudulently used accounts. Credit card companies and banks may require you to show the report in order to verify the crime when you file your initial complaint with them.
2. **Call your existing creditors and notify them that you have been a victim of identity theft** (credit cards, bank accounts, mortgages, car loans).
    a. If your existing credit accounts have been used fraudulently, request a fraud dispute form from your credit card company – if they cannot provide you with a form, you can use a form available from the FTC, a federal agency that monitors identity theft and assists consumers. To use the form, go to: http://www.consumer.gov/idtheft/pdf/affidavit.pdf.
    b. If your existing credit accounts have been used fraudulently, get replacement cards with new account numbers. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen" because it can be interpreted as though you are somehow responsible).
    c. Monitor your mail and bills for evidence of new fraudulent activity. Report it immediately to creditor grantors.
    d. Add passwords to all existing accounts and make sure that all new accounts are created with the use of a new password. This password should not be easily discovered, such as your mother's maiden name or that of one of your children, nor should it be a word that is easily guessed.

3. **Contact the fraud sections of each of the credit reporting bureaus and place a fraud alert on your credit file:**

Equifax
P.O. Box 74021
Atlanta, GA 30374-0241
To order your credit report: 1-800-685-1111
To report fraud: 1-800-525-6285

Experian
P.O. Box 9530
Allen, Texas 75013
To order your credit report: 1-800-397-3742
To report fraud: 1-888-397-3742

Trans Union
P.O. Box 390
Springfield, PA 19064-0390
To order your credit report: 1-800-916-8800
To report fraud: 1-800-680-7289

There are two types of fraud alerts, an initial alert and an extended alert. For more information, go to http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#Identity. By placing a fraud alert on your credit file, three things will be initiated:

a. Creditors will have to get your permission before opening accounts in your name.
b. Your name will be taken off pre-approved mailing lists for new credit cards.
c. You will receive a free copy of your credit report.

YOU HAVE A RIGHT TO RECEIVE A FREE COPY OF YOUR CREDIT REPORT IF:

- You are a victim of identity theft.
- You have been denied credit.
- You receive public welfare assistance.
- You are receiving unemployment benefits.
- You have not received a free credit report from each of the nationwide consumer credit reporting companies, Equifax, Experian and TransUnion, within the preceding twelve months.

ORDER YOUR CREDIT REPORT ONCE A YEAR IN ORDER TO REVIEW IT

- In a few months, you will need to order new copies of your credit reports to verify your corrections and changes.
- Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name and review your credit card statements to ensure no unauthorized charges have been made to your existing accounts.
- Since June 1, 2005, Florida residents are entitled to order a free annual credit report from each of the major credit reporting agencies in accordance with FACTA (Fair and Accurate Credit Transactions Act). To order your free reports, you can call 877-322-8228 or go to www.annualcreditreport.com.

4. **Close fraudulently created credit accounts by contacting the creditors revealed within your credit reports.**
5. **If you've had checks stolen, contact major check verification companies**. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:
    a. CheckRite -- (800) 766-2748
    b. ChexSystems -- (800) 428-9623 (closed checking accounts)
    c. CrossCheck -- (800) 552-1900
    d. Equifax -- (800) 437-5120
    e. National Processing Co. (NPC) -- (800) 526-5380
    f. SCAN -- (800) 262-7771
    g. TeleCheck -- (800) 710-9898

6. **Contact the Social Security Administration (SSA) to report fraudulent use of your SSN** such as welfare or Social Security benefit fraud. An identity thief may also be using your SSN when applying for a job. Contact the SSA at (800) 772-1213 to report the misuse and check your social security statement. To order your Earnings & Benefits Statement call (800) 772-1213. The SSA automatically mails it to individuals three months before their birthday. Web:www.ssa.gov/online/ssa-7004.html.

    To report fraud: (800) 269-0271 or write to: Social Security Administration, Office of the Inspector General, P.O. Box 17768, Baltimore, MD 21235. Web: www.ssa.gov/oig/public_fraud_reporting.

7. **Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently**. U.S. Dept. of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St., NW, Suite 500, Washington, DC 20036.
8. **You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud**. Call the Department of Highway Safety & Motor Vehicles (DHSMV) to see if another license was issued in your name. Go to your local DHSMV to request a new driver's license number. Fill out the DHSMV's complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest DHSMV investigation office.
9. Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. **If a civil judgment is entered in your name for your imposter's actions, contact the court where the judgment was entered and report that you are a victim of identity theft**. If you are wrongfully arrested or prosecuted for criminal charges, contact the police department and the court in the jurisdiction of the arrest. If the charges are in Miami-Dade County, contact the State Attorney's Office at 305-547-0100 to speak with someone in the Felony Identity Theft Unit to find out how to clear your name.

10. **Contact your telephone service provider and determine whether your telephone has remote access call forwarding features** – if so, determine whether the feature has been used – identity thieves often use this feature to intercept calls from creditors and banks when they attempt to verify the legitimacy of transactions. Thieves divert the calls to their phones and verbally authorize the transaction – the bank or creditor is left thinking that they have authorization from you – to prevent this, consider canceling this feature from your telephone account and set up a password as with all your other accounts.

11. **DON'T GIVE IN!**
    - Do not pay balances owed on any account that is the result of identity theft.
    - Do not cover any checks or pay any bank fees associated with checks that were written or cashed fraudulently.
    - Do not declare bankruptcy as a result of being defrauded – if you are declaring bankruptcy for other reasons, consult with a bankruptcy attorney regarding any fraudulent charges for which you were not responsible.
    - No legal action should be taken against you if you filed a dispute letter with the creditor.Do not let any company intimidate you or force you to pay any fraudulent accounts.Cooperate with the company's fraud investigation.

ADDITIONAL RESOURCES

- **Federal Trade Commission (FTC).** The FTC offers information for victims. File your case with the FTC Consumer Response Center. Include your police report number. Use the FTC uniform affidavit form.
  (877) ID-THEFT (877-438-4338) Web: www.consumer.gov/idtheft
- **Identity Theft Resource Center.** P.O. Box 26833, San Diego, CA 92196. Lists regional victim support groups on its web site. Offers many guides for victims. (858) 693-7935. Web: www.idtheftcenter.org
- **Identity Theft Survival Kit.** (800)725-0807. Web: www.identitytheft.org
- **Driver Privacy Protection Act ("DPPA")**
  Under Florida state law, your motor vehicle and driver license records are subject to public disclosure. DPPA allows you to **keep your personal information private** by limiting who has access to the information. DPPA is designed to limit public access to your **social security number, driver license or identification card number, name, address, and other personal information** contained in your motor vehicle and driver license records. Certain persons, organizations, businesses, and government agencies will still have access to your personal information. You can apply for an immediate block online: https://www4.hsmv.state.fl.us/dlstatus.html
- **TO REMOVE YOUR NAME FROM MAIL AND PHONE MARKETING LISTS**
  - **Direct Marketing Association**
    a. Mail Preference Service, P.O. Box 643, Carmel, NY 10512.
       Web: www.the-dma.org/consumers/offmailinglist.html
       Online opt-out program costs $5.00. It is free by mail.
    b. FTC's telemarketing Do Not Call registry (888) 382-1222
       Online registration: www.donotcall.gov

FRAUDULENT USE OF PERSONAL IDENTIFICATION INFORMATION IS A VIOLATION OF FLORIDA LAW PURSUANT TO FLORIDA STATUTE 817.568.

If there is sufficient evidence to arrest the identity thief, the matter will be presented to the State Attorney's Office for prosecution.

We hope that this information is helpful and that you always bear it in mind so that you don't become a victim of identity theft. For more information please call Community Outreach Division at 305-547-0724.