DELRAY CREDIT COUNSELING
Debt Consolidation and Credit Counseling

Identity Theft

Reviewing

What It Is
How It Happens
How To Protect Yourself
How To Recover

What is Identity Theft?

Identity theft became a very common thing in the early nineties. Since then the FTC has exercised a vast amount of resources to help to prevent it. Included in those have been several publications to help to educate consumers. The following are excerpts from the FTCs educational material.

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

1) They get information from businesses or other institutions by:
    - Stealing records from their employer,
    - Bribing an employee who has access to these records, or
    - Hacking into the organization's computers.
2) They rummage through your trash, or the trash of businesses or dumps in a practice known as "dumpster diving."
3) They obtain credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer, or someone else who may have a legal right to the information.
4) They steal credit and debit card numbers from skimming devices.
5) They steal wallets and purses containing identification and credit and bankcards.
6) They steal mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
7) They complete a "change of address form" to divert your mail to another location.
8) They steal personal information from your home.
9) They scam information from you by posing as a legitimate businessperson or government official.

Once identity thieves have your personal information, they may:

1) Go on spending sprees purchasing big-ticket items like computers that they can easily sell.
2) Open a new credit card account, using your name, date of birth, and SSN. When they don't pay the bills, the delinquent account is reported on your credit report.
3) Change the mailing address on your credit card account. The imposter then runs up charges on the account. Because the bills are being sent to the new address, it may take some time before you realize there's a problem.
4) Take out auto loans in your name.
5) Establish phone or wireless service in your name.
6) Counterfeit checks or debit cards, and drain your bank account.
7) Open bank accounts in your name and write bad checks on that account.

How you can tell if you're a victim of identity theft?

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

1) Failing to receive bills or other mail signaling an address change by the identity thief.
2) Receiving credit cards for which you did not apply;
3) Denial of credit for no apparent reason; or
4) Receiving calls from debt collectors or companies about merchandise or services you didn't buy.

What You Should Do

Call the toll-free fraud number of anyone of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

· **Equifax** — To report fraud, call: 1-800-525-6285,
· **Experian** — To report fraud, call: 1-888-EXPERIAN
· **TransUnion** — To report fraud, call: 1-800-680-7289

Once you receive your reports, review them carefully. Look for inquiries you didn't initiate, accounts you didn't open, and unexplained debts on your true accounts. You also should check that information such as your SSN, addresses, name or initial, and employers are correct. Inaccuracies in this information also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, you should notify the credit bureau as soon as possible by telephone and in writing. You should continue to check your reports periodically, especially in the first year after you've discovered the theft, to make sure no new fraudulent activity has occurred. The automated "one-call" fraud alert process only works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alerts must be made separately at each of the three major credit bureaus.

Protecting Against Identity Theft

As with any crime, you can't guarantee that you will never be a victim, but you can minimize your risk. By managing your personal information widely, cautiously and with an awareness of the issue, you can help guard against identity theft.

- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. You can check the organization's Web site as many companies post scam alerts when their name is used improperly, or you can call customer service using the number listed on your account statement or in the telephone book.
- Don't carry your SSN card; leave it in a secure place.
- Secure personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Guard your mail and trash from theft:
- Carry only the identification information and the number of credit and debit cards that you'll actually need.

- Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect personally identifying information from you. 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 if you can keep your information confidential.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your account number.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work as well as any copies you may keep of administrative forms that contain your sensitive personal information.
- Cancel all unused credit accounts.
- When ordering new checks, pick them up at the bank, rather than having them sent to your home mailbox.

What You Should Do If Your Identity is Stolen?

If your information or identification documents were stolen or scammed, you have an opportunity to prevent the misuse of that information if you can take action quickly.

- For financial account information such as credit card or bank account information: Close those accounts immediately. When you open new ones, place passwords on these accounts. Avoid using your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- For SSN: Call the toll-free fraud number of any one of the three major credit bureaus and place a fraud alert on your credit reports. This can help prevent an identity thief from opening new credit accounts in your name.
- To replace an SSN card: Call the Social Security Administration at 1-800-772-1213 to get a replacement.
- For driver's license or other identification documents: Contact the issuing agency. Follow their procedures to place fraud flags and to get replacements.

Once you have taken these precautions, there really isn't anything more you need to do except to check for the signs that your information is being misused. See "How can I tell if I'm a victim of identity theft?" Are there any other steps I can take to make sure I'm not an identity theft victim? You don't have to file an identity theft report with the police or with the FTC until you find out if your information is actually being misused. If another crime was committed, such as theft of your purse or wallet or your house or car was broken into, report that crime to the police.

Recovering From Identity Theft

The Fair Credit Billing Act (FCBA) establishes procedures for resolving billing errors on your credit card accounts, including fraudulent charges on your accounts and limits your liability for unauthorized credit card charges to $50 per card. To take advantage of the law's consumer protections, you must:

- Write to the creditor at the address given for "billing inquiries," not the address for sending your payments. Include your name, address, account number and a description of the billing error, including the amount and date of the error.
- Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If the address on your account was changed by an identity thief; and you never received the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is why it's so important to keep track of your billing statements and immediately follow up when your bills don't arrive on time.
- Send your letter by certified mail, and request a return receipt. This will be your proof of the date the creditor received the letter. Include copies (NOT originals) of sales slips or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

Delray Credit Counseling Corp.
5300 West Atlantic Ave. Suite 200
Beach Florida 33484
(800) 982-8445