Avoid Getting Weighed Down by

Identity Theft

What is identity theft?

Identity theft occurs when someone uses your personally identifying information without your permission, such as: your name, social security number, credit card numbers, or other financial account information. Once obtained, the information is used to commit fraud or other crimes. The FTC estimates that as many as 9 million Americans have their identities stolen each year. Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record.

How do thieves steal an identity?

Skilled thieves may use a variety of methods to get hold of your information, including:

- **Changing Your Address:** A diversion of your billing statements to another location by completing a change of address form.
- **Dumpster Diving:** Thieves will rummage through trash looking for bills or other paper with your personal information on it. That's why it's important to shred documents with your personal information before it goes to the trash.
- **Old-fashioned Stealing:** Perpetrators steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They can also steal personnel records, or bribe employees who have access.
- **Phishing:** This occurs when thieves contact you disguised at financial institutions or companies. Sometimes phishing comes in the form of spam or pop-up messages to get you to reveal your personal information.
- **Pretexting:** The use of false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
- **Skimming:** Typically an "inside job" by a dishonest employee of a legitimate merchant. The thief can procure a victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' credit card numbers.

How can you find out if your identity has been stolen?

The best way to find out is to monitor your accounts and bank statements each month, and checking your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. Unfortunately, many consumers learn that their identity has been stolen after some damage has been done, such as:

- When bill collection agencies contact you for overdue debts you never incurred.
- When making application for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- Receiving something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

For more information regarding Identity Theft, visit the Federal Trade Commission Website: ftc.gov

stewart™ TITLE

4 Steps to Take as a Victim of Identity Theft

If you are a victim of identity theft, take the following four steps as soon as possible. Keep a record with the details of your conversations and copies of all correspondence. Acting fast could mean a huge difference in the time it will take to restore you good name.

Step 1: Place a Fraud Alert

Nip the problem where it hurts, review your credit reports, place a fraud alert and prevent further damage. A fraud alert can help prevent an identity thief from opening any more accounts in your name. Contact any one of the three consumer reporting companies below to place a fraud alert on your credit report.

- **Equifax**.....1.888.766.0008 ....equifax.com
- **Experian** .....1.888.397.3742 .....experian.com
- **TransUnion** ..1.888.909.8872.....transunion.com

It's only necessary to contact one of the reporting companies, since they contact each other in this situation, but it is necessary to receive a confirmation of your fraud alert from all three. Once your fraud alert is filed, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies. Evaluate any suspicious activity you see on your current reports and continue to check your credit reports periodically for new fraudulent activity, especially for the first year after you discover the identity theft. There are two different types of fraud alerts that you can file.

- Initial Fraud Alert - This alert stays on your credit report for at least 90 days. This kind of alert is appropriate if your wallet has been stolen or if you've been taken in by a phishing scam. With an initial fraud alert, potential creditors must use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name.
- Extended Fraud Alert - Stays on your credit report for seven years. This kind of alert is appropriate if you have actually become a victim of identity theft and can provide the consumer reporting company with an Identity Theft Report. Potential creditors must actually contact you, or meet with you in person, before they issue credit in your name. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you request to have your name back on the lists before then.

Step 2: Closing Accounts

Close the accounts that you know, or believe, have been tampered with or opened fraudulently. It is important to close and re-open tarnished accounts to prevent further problems. Contact someone in the security or fraud department of each company and request the proper forms to dispute charges and debits on your accounts or fraudulently opened accounts. Follow up in writing, and include copies (not originals) of supporting documents. Document everything and Keep a file of your correspondence and enclosures: Send letters by certified mail, return receipt requested, so you can document what the company received and when. Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

Step 3: File a Complaint with the Federal Trade Commission

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

- **Federal Trade Commission**
  1.877.ID.THEFT (438.4338)
  ftccomplaintassistant.gov

Step 4: File a Local Police Report

Call your local police and request instructions for filing an identity theft or "miscellaneous incident" report in person (preferable), by phone, or online. When you visit your local police department to file your report, bring a printed copy of your FTC ID Theft Complaint form, your cover letter and your supporting documentation. Ask the officer to attach or incorporate the complaint form into their police report to provide full documentation of the incident. Keep originals of every report, or form filed for your own records.

stewart TITLE