

Identity Theft:

How to Protect Yourself and What to Do If You Are a Victim



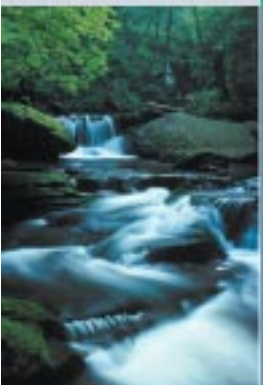
Congratulations! By reading this publication you've taken the first step towards protecting yourself against identity theft. This publication is brought to you by TrueCredit, a leading provider of credit monitoring, reporting and scoring tools. Myvesta has chosen to partner with TrueCredit to bring you credit-based products and services that go beyond the delivery of credit data. TrueCredit's monitoring program allows you to monitor your credit report to protect yourself from unauthorized changes and loss from identity theft.

Credit Monitoring can be purchased online through Myvesta.org. You will receive a credit report, weekly email alerts to changes in your credit report, credit trending and access to Fraud Resolution Services to help you recover from losses resulting from identity theft.

We hope you find the information in this publication to be useful and helpful. If you would like to protect yourself from identity theft with Credit Monitoring, visit Myvesta.org.

Introduction

Think your money and peace of mind are safe from thieves? Think again. Identity theft is one of the fastest growing types of robbery today. As many as 300,000 people are defrauded each year by crooks using stolen identities. Guess who ends up paying for the millions of



► Myvesta is a nonprofit consumer education organization. We provide a wide range of educational materials to assist those in financial need. Visit us on the Web at Myvesta.org.

dollars that stores and lending institutions lose in this way? That's right. You and me.

Identity theft occurs when a thief gets your identifying information and poses as you to run up your credit cards, open new credit cards and bank accounts, drain bank accounts, apply for jobs and housing, get loans, open utilities and long distance phone accounts, get false identities and write false checks. Identity thieves can even commit crimes then give their fake identity (your name) to police when they are arrested.

Unfortunately, the way that most people discover that their identity has been stolen is by getting a collection call from a company they never did business with or by being denied a loan because of a bad credit rating, when they have always paid their bills on time. Although the victim of identity theft may not be responsible for the actual debt, he or she may be left with a bad credit report that can take years to correct. This bad credit report affects a consumer in every facet of his life — the ability to get loans, the cost of insurance, mortgages, bank accounts, rent apartments and it can even destroy job chances. Victims spend hundreds of hours and thousands of dollars straightening out their credit records.

Thankfully, Congress listened to the victims of identity theft and, in October 1998, enacted the Identity Theft and Assumption Deterrence Act. The Act gives victims a weapon against identity thieves and a single place where they can file a complaint and get consumer information. The Federal Trade Commission maintains a Web site where victims of identity theft can file a complaint at www.ftc.gov. It

also criminalizes fraud in connection with theft and misuse of personal identifying information. Anyone who steals another person's identity, and gains \$1,000 within one year from

misusing that identity, is subject to a fine and imprisonment of up to 20 years.

Some states have also criminalized identity theft. Check your consumer protection or consumer affairs office to see if your state has such a law and how it can help you.

How does a thief get my identity information?

It is very easy for a thief to get important information from you. A thief can get information from you by:

- ▶ Reaching into your mailbox and sifting through your mail and stealing your bills, credit card applications, pre-approved cards, bank or credit card statements or credit cards
- ▶ Looking through your trash for credit or debit card slips, checks, credit card applications or other documents with identifying information
- ▶ Stealing your wallet
- ▶ A merchant's employee stealing your identification from a check or credit card slip
- ▶ Filling out a change of address card to divert your mail to the thief's address
- ▶ Relatives, roommates, friends, household workers, ex-spouses using your identity without your authority
- ▶ Obtaining a copy of your credit report by pretending to be someone with a "legitimate business purpose" to the information under the Fair Credit Reporting Act
- ▶ Watching you punch in your Personal Identification Number ("PIN") at ATMs or public telephones

The personal information that thieves want and that you should be very careful about protecting is: your Social Security Number, your mother's maiden name, your passwords

Anyone who steals another person's identity, and gains \$1,000 within one year from misusing that identity, is subject to a fine and imprisonment of up to 20 years.

and PINs for debit and long distance telephone cards, credit card numbers, old and current addresses and your birth date.

How can I prevent identity thieves from getting my information?

Identity theft is prevalent because it is so easy to do and so hard to detect. You can be proactive to make it harder for thieves to get your personal information and easier for you to detect fraudulent activity early on. Taking proactive steps is especially important because it is so difficult to erase the false information from all your identifying documents, such as your credit report. The following steps will help you police your information and reduce the overall information that is available on you:

- ▶ Pay attention to your billing cycles and contact creditors if bills do not arrive on time. Also, know when new or reissued credit cards will be coming in the mail.
- ▶ Leave all unnecessary documents at home, including excess credit cards or identification (such as your birth certificate or passport).
- ▶ Keep documents with personal information, like canceled checks, in a safe place and shred them when you don't need them anymore. Documents that you should shred include charge

receipts, copies of credit applications, insurance forms, bank checks and statements and old charge or debit/ATM cards.

- ▶ Document all important creditor information — contact information, account numbers, expiration dates and any other relevant information — and keep it in

Documents that you should shred include charge receipts, copies of credit applications, insurance forms, bank checks and statements and old charge or debit/ATM cards.

a safe place in your home.

- ▶ Don't dispose of identifying information, like an ATM, debit card or credit card slip, in a public trash can.
- ▶ Cancel all unused credit card accounts so that an identity thief cannot get these account numbers from your credit report.
- ▶ Consider opting out of pre-approved offers of credit by removing your name from the marketing lists of the three major credit reporting agencies, Equifax, Trans Union and Experian. To take yourself off the lists of all three reporting agencies, call 1-888-5OPTOUT (1-888-567-8688).
- ▶ Consider signing up for the Direct Marketing Association's Mail and Telephone Preference Services. Write to the following addresses and ask to be added to "name deletion lists" to stop mail and telemarketing.

Mail Preference Service

P.O. Box 9008
Farmingdale, NY 11735-9008
www.dmaconsumers.org/offmailinglist.html

Telephone Preference Service

P.O. Box 9014
Farmingdale, NY 11735-9014
www.dmaconsumers.org/offmailinglist.html

- ▶ Consider having your name and address removed from the phone book and directories. Contact your local telephone company to find out how to get an unlisted telephone number.
- ▶ Use a mailbox that is locked or contact the post office to get a post office box to deter thieves from stealing your mail.
- ▶ Always pick up newly ordered checks at the bank to avoid having blank checks in your mailbox.

- ▶ Be sure to mail all paid bills at the post office or use a public mail box.
- ▶ Be smart when giving personal information over the phone. If you have any doubts about the person asking the information, hang up and initiate the call yourself.
- ▶ Check your credit report annually. You can get a consolidated report from all three major credit reporting agencies at Myvesta.org. Fill out the investigation form if you find any inaccuracies that you want to dispute.
- ▶ Be smart when picking a Personal Identification Number (“PIN”) or password. Thieves assume you’ll use a number that is easy to remember, like the last four digits of your Social Security number or your birth date. Don’t have your PIN written on your card.
- ▶ Make sure no one can see you punch in your PIN or password at the ATM or retailer, or your telephone card number at a public telephone.
- ▶ Be protective of your Social Security number (“SSN”). If someone asks for it, such as when you write a check, see if you can provide another number. There are some forms where it is necessary, such as your tax forms.

What should I do if my identity is stolen?

If your identity is stolen, you have to take steps to ensure that the thief can no longer pose as you and to restore your credit history and good name. Fortunately, you may not be responsible for debt that a thief incurs using your name. (If an identity thief runs up credit cards in your name, and you notify your creditors, the most that you will be responsible for is the first \$50

Fortunately, you may not be responsible for debt that a thief incurs using your name.

that was fraudulently charged. The same is generally true of debit cards. See Myvesta’s publication “When is a Credit Card Not a Credit Card? Credit Card or Debit Card, the Great Debate”). If your identity has been stolen, you should do the following IMMEDIATELY:

- ▶ Notify creditors by phone as soon as you discover the theft. Ask for the fraud department and have them close all your accounts. Follow up with a certified letter, return receipt requested, confirming your telephone call.
- ▶ Contact the major credit reporting agencies to ask that a “fraud alert” be placed in your file.

Experian — experian.com

Trans Union — tuc.com

Equifax — equifax.com

Add a “victim’s statement” explaining that your identity was stolen. This statement may be placed in your file for a limited period of time, so be sure to renew it if necessary.

- ▶ Call the local police and report the fraud. Some banks or credit card companies may require you to show a police report to verify the crime.
- ▶ Call your bank/credit union and cancel old account numbers, PINs, ATM and debit cards, and get new ones. You should report false checks/bank accounts to the following check guarantee companies so that they will flag your file and ensure counterfeit checks will be refused:

TeleCheck

1-800-710-9898

International Check Services

1-800-526-5380

Equifax

1-800-437-5120

- ▶ If you suspect that someone is using your driver's license number, call the Department of Motor Vehicles ("DMV"). The DMV can tell you if it issued another license in your name. If this is the case, get a new number and ask the DMV to investigate the identity theft. You may have to fill out a form. Some DMVs allow you to block your information from being released.
- ▶ Call all utilities (electrical, gas, water, local telephone, long distance telephone and cable TV) and let them know that other services may have been fraudulently requested in your name. You may need to change account and telephone numbers.
- ▶ If your SSN was used fraudulently, report the problem to the Social Security Administration's Fraud Hotline 1-800-269-0271. In extreme cases of fraud, you may be able to get a new SSN. At the same time, don't impulsively change your SSN as it can put burdens on you later.
- ▶ Mail fraud victims should contact their local Postal Inspection Service Office.
- ▶ An identity thief may order a passport in your name. Send a certified letter, return receipt requested, to the passport office to let it know someone may pose as you to order a new passport in your name.

These steps may seem drastic, but you must be careful — don't think you're safe because you canceled your credit card and placed a stop on your checking account. Once identity thieves have your identification information, they can open new bank, credit card, utility and other accounts and lines of credit under your name.

You should keep a log of everything you do to correct the identity theft. Write down all telephone conversations in detail — date and time, name of person with whom you speak, telephone numbers and the substance of the conversation. See the sample log on last page

of this publication. Send all letters by certified mail, return receipt requested. Keep copies of all letters and documents.

Under the law, the Identity Theft and Assumption Deterrence Act of 1998, you can notify the Federal Trade Commission, which keeps a database of all complaints.

Call 1-877-IDTHEFT (1-877-438-4338) to receive consumer information and get referrals to the appropriate organization that you should contact.

About Myvesta...

Myvestasm is dedicated to helping people create healthy financial lives. The organization provides a wide range of materials to inspire and inform people so they can break down their barriers to financial and personal success. For more information visit Myvesta.org online.

Information Guarantee

The information in this publication is updated frequently. If you have not downloaded this publication directly from Myvesta.org, visit Myvesta.org to download a current copy of this publication.

We hope you find the information in this publication helpful. Please understand that Myvesta.org's publications are not intended to be legal, investment or financial planning advice. You should contact a lawyer, investment advisor, financial planner or other licensed professional in your state for specific advice.

Telephone Conversation Log

Date: _____ **Conversation With:** _____

Telephone Number(s): _____

Notes: _____

Date: _____ **Conversation With:** _____

Telephone Number(s): _____

Notes: _____

Date: _____ **Conversation With:** _____

Telephone Number(s): _____

Notes: _____

Date: _____ **Conversation With:** _____

Telephone Number(s): _____

Notes: _____

Date: _____ **Conversation With:** _____

Telephone Number(s): _____

Notes: _____
