What's It All About?

Federal Trade Commission
May 2003

Dear Consumer:

The Federal Trade Commission has published this booklet to help raise consumer awareness of identity theft.

If you or someone you know is a victim of identity theft, please visit www.consumer.gov/idtheft. The information you enter there becomes part of a secure database that's used by law enforcement officials across the nation to help stop identity thieves. The site also has links to useful information from other federal agencies, states and consumer organizations.

You also may want to call 1-877-ID THEFT, the FTC's toll-free ID Theft Hotline, where counselors help consumers who want or need more information about dealing with the consequences of identity theft.

We encourage you to share this booklet with your family, friends, colleagues and neighbors.

Sincerely,

J. Howard Beales, III
Director
Bureau of Consumer Protection
Federal Trade Commission

Contents

Letter to Consumers

Introduction 1

How Identity Theft Occurs 2

How Can I Tell if I'm a Victim of Identity Theft? 5

Managing Your Personal Information 6

A Special Word About Social Security Numbers 9

If Your Identity's Been Stolen 12

FTC Privacy Policy 18

Introduction

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trade? Your everyday transactions, which usually reveal bits of your personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address and phone numbers. An identity thief obtains some piece of your sensitive information and uses it without your knowledge to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and their hard-earned money – cleaning up the mess the thieves have made of their good name and credit record. Some victims have lost job opportunities, been refused loans for

education, housing or cars, or even been arrested for crimes they didn't commit.

Can you prevent identity theft from occurring? As with any crime, you cannot completely control whether you will become a victim. But, according to the Federal Trade Commission (FTC), you can minimize your risk by managing your personal information cautiously and with heightened sensitivity.

How Identity Theft Occurs

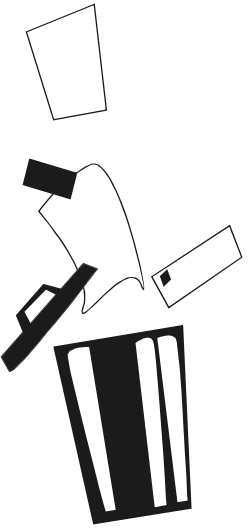
Skilled identity thieves use a variety of methods to gain access to your personal information. For example:

- 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.

- They rummage through your trash, the trash of businesses, or dumps in a practice known as "dumpster diving."

- 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.



- 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 mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.

- They complete a "change of address form" to divert your mail to another location.

- They steal personal information from your home.

- They scam information from you by posing as a legitimate business person or government official.

Once identity thieves have your personal information, they may:

- Go on spending sprees using your credit and debit card account numbers to buy

"big-ticket" items like computers that they can easily sell.

- 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.

- 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.

- Take out auto loans in your name.

- Establish phone or wireless service in your name.

- Counterfeit checks or debit cards, and drain your bank account.

- Open a bank account in your name and write bad checks on that account.

- File for bankruptcy under your name to avoid paying debts they've incurred, or to avoid eviction.

- Give your name to the police during an arrest. If they are released and don't show up for their court date, an arrest warrant could be issued in your name.

How Can I Tell if I'm a Victim of Identity Theft?

Indications of identity theft can be:

- failing to receive bills or other mail signaling an address change by the identity thief;
- receiving credit cards for which you did not apply;
- denial of credit for no apparent reason; or
- receiving calls from debt collectors or companies about merchandise or services you didn't buy.

Order a copy of your credit report from each of the three major credit bureaus. If it's accurate and includes only those activities you've authorized, chances are you're not a victim of identity theft. The law allows credit bureaus to charge you up to $9 for a copy of your credit report.

To order your credit reports:

Equifax – www.equifax.com
1-800-685-1111
Experian – www.experian.com
1-888-EXPERIAN (397-3742)
TransUnion – www.transunion.com
1-800-916-8800

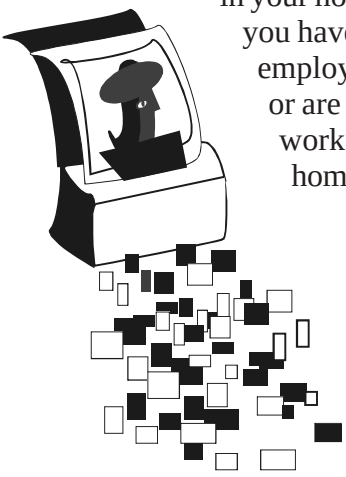
Managing Your Personal Information

So how can a responsible consumer minimize the risk of identity theft, as well as the potential for damage? When it involves your personal information, exercise caution and prudence.

Do It Now

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 you're asked for your mother's maiden name on an application for a new account, try using a password instead.

Secure personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home.



Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that your records are kept in a secure location. Ask about the disposal procedures for those records as well.

Everyday Diligence

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 can be skilled liars, and may pose as representatives of banks, Internet service providers (ISPs) or even government agencies to get you to reveal identifying information. Before you divulge any personal information, confirm that you're dealing with a legitimate representative of a legitimate organization. Double check by calling customer service using the number on your account statement or in the telephone book.

Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail from your mailbox promptly. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to ask for a vacation hold. To thwart a thief who may pick through your trash or recycling

bins, tear or shred your charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements, and expired charge cards.

Before revealing any identifying information (for example, on an application), ask how it will be used and secured, and whether it will be shared with others. Find out if you have a say about the use of your information. For example, can you choose to have it kept confidential?

Keep your Social Security card in a secure place and 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.

Limit the identification information and the number of credit and debit cards that you carry to what you'll actually need.

Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address.

Keep your purse or wallet in a safe place at work.

A Special Word About Social Security Numbers

Very likely, your employer and financial institution will need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. If someone asks for your SSN, ask the following questions:

- Why do you need it?
- How will it be used?
- How do you protect it from being stolen?
- What will happen if I don't give it to you?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to your questions will help you to decide whether you want to share your SSN with the business.

Consider Your Computer

Your computer can be a goldmine of personal information to an identity thief. Here's how you can safeguard your computer and the personal information it stores:

- Update your virus protection software regularly. Computer viruses can have damaging effects, including introducing program code that causes your computer to send out files or other stored information. Look for security repairs and patches you can download from your operating system's Web site.

- Don't download files from strangers or click on hyperlinks from people you don't know. Opening a file could expose

your system to a computer virus or a program that could hijack your modem.

- Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. The firewall allows you to limit uninvited access to your computer. Without a firewall, hackers can take over your computer and access sensitive information.

- Use a secure browser – software that encrypts or scrambles information you send over the Internet – to guard the safety of your online transactions. When you're submitting information, look for the "lock" icon on the status bar. It's a symbol that your information is secure during transmission.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a "strong" password – that is, a combination of letters (upper and lower case), numbers and symbols.

  Avoid using an automatic log-in feature that saves your user name and password; and always log off when you're finished. If your laptop gets stolen, the thief will have a hard time accessing sensitive information.

- Delete any personal information stored on your computer before you dispose of it. Use a "wipe" utility program, which

overwrites the entire hard drive and makes the files unrecoverable.

- Read Web site privacy policies. They should answer questions about the access to and accuracy, security and control of personal information the site collects, as well as how sensitive information will be used, and whether it will be provided to third parties.

If Your Identity's Been Stolen

Even if you've been very careful about keeping your personal information to yourself, an identity thief can strike. If you suspect that your personal information has been used to commit fraud or theft, **take the following four steps right away**. Remember to follow up all calls in writing; send your letter by certified mail, return receipt requested, so you can document what the company received and when; and keep copies for your files.

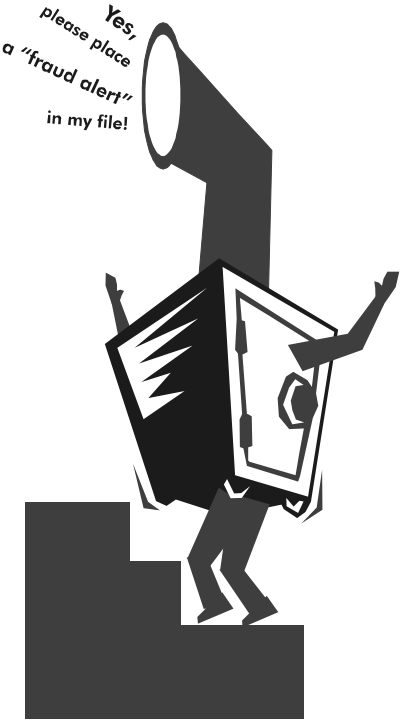
1. Contact the fraud departments of each of the three major credit bureaus.

- **Equifax –** To report fraud, call: 1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241

- **Experian –** To report fraud, call: 1-888-EXPERIAN (397-3742), and write: P.O. Box 9532, Allen, TX 75013

- **TransUnion –** To report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Tell them you're a victim of identity theft, and ask them to place a "fraud alert" in your file, as well as a "victim statement." It's a signal to creditors to call you before they open any new



accounts or change your existing accounts, and helps prevent an identity thief from opening additional accounts in your name. At the same time, order copies of your credit reports. Credit bureaus must give you a free copy of your report if it's inaccurate because of fraud **and** you send them a written request.

Check your credit reports carefully to make sure the information is accurate. 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, address(es), name or initial, and employers are correct. Inaccuracies also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, notify the credit bureau as soon as possible by telephone and in writing. In a few months, order new copies of your reports – both to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

"Fraud alerts" and "victim statements" are primarily voluntary services of the credit bureaus. Creditors do not have to consider them when granting credit. That's one more reason to check your credit reports regularly. In addition, fraud alerts and victim statements expire;

you need to renew them periodically. Ask each credit bureau about its policy.

2. Close any accounts that have been tampered with or opened fraudulently.

Credit Accounts

Credit accounts include all accounts with banks, credit card companies and other lenders, and phone companies, utilities, ISPs, and other service providers.

If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords.

If there are fraudulent charges or debits, ask the company about the following forms for disputing those transactions:

For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (available at **www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf**). If they don't, ask the representative to send you the company's fraud dispute forms.

For your existing accounts, ask the representative to send you the company's fraud dispute forms.

If your ATM card has been lost, stolen or otherwise compromised, cancel the

card as soon as you can. Get a new card with a new PIN.

Checks

If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. While no federal law limits your losses if someone steals your checks and forges your signature, state laws may protect you. Most states hold the bank responsible for losses from a forged check, but they also require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely way that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

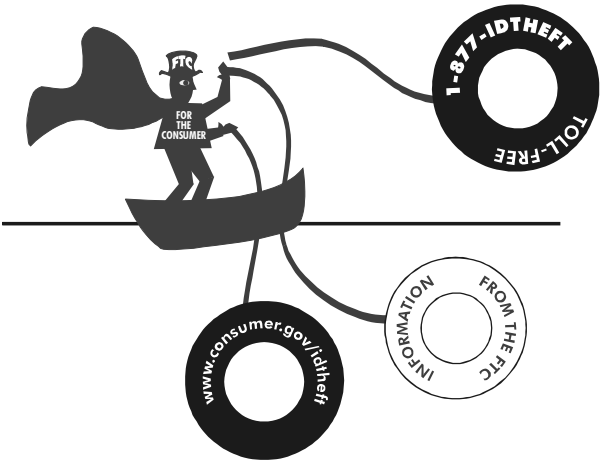
You also should contact these major check verification companies. Ask that retailers who use their databases not accept your checks.

TeleCheck –
1-800-710-9898 or 927-0188

Certegy, Inc. –
1-800-437-5120

International Check Services –
1-800-631-9656

Call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.



3. File a report with your local police or the police in the community where the identity theft took place.

Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

4. File a complaint with the FTC.

Visit **www.consumer.gov/idtheft** to file a complaint instantly, obtain a copy of the ID Theft Affidavit and get answers to frequently asked questions about identity theft. If you don't have access to the Internet, call the FTC's Identity Theft Hotline, toll-free, at 1-877-IDTHEFT (438-4338). Your complaint will be entered into a secure consumer fraud database, accessible only to law enforcement agencies, for use in pursuing criminal investigations.

FTC PRIVACY POLICY

The FTC enters the information you provide into our secure database – the Identity Theft Clearinghouse – and it is shared with our attorneys and investigators. It also may be shared with employees of various federal, state, or local law enforcement or regulatory authorities. We also may share information with certain private entities, such as credit bureaus and any companies you may have complained about when we believe that doing so might help resolve identity theft-related problems. You may be contacted by the FTC or any of the agencies or private entities to which your complaint has been referred. In other limited circumstances, including requests from Congress, we may be required by law to disclose information you submit.

You have the option to submit your information anonymously. However, if you do not provide your name and contact information, law enforcement and other entities will not be able to contact you for additional information to assist in their investigations and prosecutions.

1-877-ID-THEFT (1-877-438-4338)

www.consumer.gov/idtheft