ID THEFT:
What It's All About

Federal Trade Commission
June 2005

Dear Consumer:

The Federal Trade Commission has published this booklet to help raise awareness of identity theft. We encourage you to share it with your family, friends, colleagues, and neighbors.

If someone has used your name or other personal information to commit a fraud, please visit **www.consumer.gov/idtheft** for information on how to proceed and how to file an identity theft complaint. The site has links to useful information from other federal agencies, states, and consumer organizations. The information in your complaint becomes part of a secure database that law enforcement officials across the nation use to help stop identity thieves.

If you don't have access to the Internet, call 1-877-ID-THEFT, the FTC's toll-free ID Theft Hotline.

Sincerely,

Lydia B. Parnes

Lydia B. Parnes, Director
Bureau of Consumer Protection
Federal Trade Commission

TABLE OF CONTENTS

Letter to Consumers

Introduction..... 1

How Identity Theft Occurs..... 2

How Can You Tell if You're a Victim
of Identity Theft?..... 5

Getting Your Credit Report..... 6

Managing Your Personal Information..... 8

A Special Word About Social
Security Numbers..... 13

Active Duty Fraud Alerts..... 14

If Your Personal Information
Has Been Lost or Stolen..... 15

Identity Theft Victims:
Immediate Steps..... 17

Fraud Alerts..... 19

Identity Theft Reports..... 20

For More Information..... 24

FTC Privacy Policy..... 25

INTRODUCTION

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, change service providers for your cell phone, or apply for a credit card. In each transaction, you reveal bits of personal information, like your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address, and phone numbers – a goldmine of information for an identity thief. Once a thief has that information, it can be used without your knowledge to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend time and money cleaning up the mess the thieves have made of their good name and credit record. They may lose out on job opportunities, and loans for education, housing, or cars. They may even get arrested for crimes they didn't commit.

Can you prevent an identity theft? As with any crime, you cannot completely control whether you will become a victim. But according to the Federal Trade Commission (FTC), the nation's consumer protection agency, you can minimize your risk by managing your personal information cautiously.

HOW IDENTITY THEFT OCCURS

Skilled identity thieves use a variety of ways to gain access to your personal information. For example, they may get information from businesses or other institutions by stealing it while they're on the job; bribing an employee who has access to these records; hacking these records; and conning information out of employees. Or:

- they may steal your wallet or purse.
- they may steal your personal information through email or the phone by saying they're from a legitimate company and claiming that you have a problem with your account. This practice is known as "phishing" online, or "pretexting" by phone.
- they may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach a device to an ATM machine where they may enter or swipe your card.
- they may get your credit reports by abusing the authorized access that was granted to their employer, or by posing as a landlord, employer, or someone else who may have a legal right to your report.
- they may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."

- they may steal personal information they find in your home.

- they may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.

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

Once identity thieves have your personal information, they may use it to commit fraud or theft. For example:

- they may call your credit card issuer to change the billing address on your account. The imposter then runs up charges on your account. Because the bills are being sent to a different address, it may be some time before you realize there's a problem.

- they may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.

- they may establish phone or wireless service in your name.

- they may open a bank account in your name and write bad checks on the account.

- they may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.

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

- they may buy a car by taking out an auto loan in your name.

- they may get identification such as a driver's license issued with their picture, in your name.

- they may get a job or file fraudulent tax returns in your name.

- they may give your name to the police during an arrest. If they don't show up for the court date, a warrant for arrest is issued in your name.

HOW CAN YOU TELL IF YOU'RE A VICTIM OF IDENTITY THEFT?

If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from the three nationwide consumer reporting companies. If you have lost any personal information – or if it has been stolen – you may want to check all your reports more frequently for the first year.

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

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

GETTING YOUR CREDIT REPORT

FREE ANNUAL CREDIT REPORTS
An amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months.

Free reports have been phased in during a nine-month period, starting with states in the West and ending with states in the East. Beginning September 1, 2005, free reports will be accessible to all Americans, regardless of where they live.

To order your free annual report from one or all the national consumer reporting companies, visit: **www.annualcreditreport.com**; call toll-free: 877-322-8228; or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from **ftc.gov/credit**. Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through **www.annualcreditreport.com**, 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

OTHER RIGHTS TO FREE REPORTS
Under federal law, you're also entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you request

your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company that supplied the information about you. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to $10.50 for additional copies of your report.

TO BUY A COPY OF YOUR REPORT, CONTACT:

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

Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports.

If you ask, only the last four digits of your Social Security number will appear on your credit reports.

MANAGING YOUR PERSONAL INFORMATION

How can a responsible consumer minimize the risk of identity theft, as well as the potential for damage? When a situation 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 open new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask to use a password instead.

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

Ask about information security procedures in your workplace or at businesses, doctors' offices, or other institutions that collect your personally identifying information. 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 information will be shared with anyone else. If so, ask how your information can be kept confidential.

EVERYDAY DILIGENCE

Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you're dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it in. Many companies post scam alerts on their sites when their name has been used improperly. Or call customer service using the number listed on your account statement or in the telephone book.

Treat your mail and trash carefully. Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. 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 request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

To thwart a thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts,

copies of credit applications, insurance forms, physician statements, checks and bank statements, expired credit or charge cards that you're discarding, and credit offers you get in the mail. To opt out of receiving offers of credit in the mail that are based on your credit report, call: 1-888-5-OPTOUT (1-888-567-8688). The nationwide consumer reporting companies use the same toll-free number to let you opt out of receiving credit offers based on their lists. **Note:** You will be asked to provide your SSN, which the consumer reporting companies need to match you with your file.

Don't carry your SSN card in your wallet; store it in a secure place.

Give your SSN only when absolutely necessary, and ask to use other types of identifiers. 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 policy number.

Carry only the identification information and the credit and debit cards that you'll actually need when you go out. If your wallet is stolen – or if you lose it – report it immediately to the card issuers and the local police.

Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.

Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

When ordering new checks, pick them up from the bank instead of having them mailed to your home.

CONSIDER YOUR COMPUTER

Your computer can be a goldmine of personal information to an identity thief. Here are some ways to help you keep your computer – and the personal information it stores – safe.

- Update your virus protection software regularly; install patches for your operating system and other software programs to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. Ideally, you should set your virus protection software to update automatically. The Windows XP operating system also can be set to check for patches automatically and download them to your computer.

- Do not open files sent to you by strangers, click on hyperlinks, or download programs from people or companies you don't know. Be cautious about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.

- Use a firewall program, especially if you use a high speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program allows you to stop uninvited access to your computer.

Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.

- If you need to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for secure). Unfortunately, no indicator is foolproof; some fraudulent sites have forged security icons.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use what experts call a "strong" password – a combination of letters (upper and lower case), numbers, and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. If your laptop is stolen, it makes it harder for a thief to access your personal information.

- Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.

- Look for website privacy policies, and read them. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.

A SPECIAL WORD ABOUT SOCIAL SECURITY NUMBERS

Your employer and financial institutions need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SSN for general recordkeeping. If someone asks for your SSN, ask:

- 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. The decision to share is yours.

ACTIVE DUTY FRAUD ALERTS

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports by contacting any one of the three major consumer reporting companies. Active duty alerts can help minimize the risk of identity theft while you are deployed. To place an alert on your credit report, or to have it removed, you will have to provide appropriate proof of your identity, including your SSN, name, address, and other personal information requested by the consumer reporting company. You may use a personal representative to place or remove an alert.

Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When a business sees the alert on your credit report, they must verify your identity before issuing any credit. As part of this verification process, the business may try to contact you directly. Be sure to keep your contact information updated, or you may experience delays if you are applying for new credit.

When you place an active duty alert on your credit report, you'll also be removed from the credit reporting companies' marketing list for prescreened credit card offers for two years unless you ask to be put back on the list before then.

IF YOUR PERSONAL INFORMATION HAS BEEN LOST OR STOLEN

If you've lost personal information or identification, or if it has been stolen from you, you can minimize the potential for identity theft if you act quickly.

- **Financial accounts:** Close accounts, like credit card and bank accounts, immediately. When you open new accounts, place passwords on them. 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.

- **Social Security number:** Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports (see page19). An alert can help stop someone from opening new credit accounts in your name.

- **Driver's license/other government-issued identification:** Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you have taken these precautions, watch for signs that your information is being misused, and that your identity has been stolen.

If your information has been misused, file a report about the theft with the police, and file a complaint with the FTC, as well. If another crime was committed – for example, if your purse or wallet was stolen or your house or car was broken into – report it to the police immediately.

IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

If you are a victim of identity theft, take the following four steps as soon as possible, and keep records of your conversations and copies of all correspondence. You also should get a copy of the FTC publication, *Take Charge: Fighting Back Against Identity Theft*, a comprehensive guide that describes what to do, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future. The guide also includes the ID Theft Affidavit to help you report information to many companies. For more information, see **www.consumer.gov/idtheft**.

1. **Place a fraud alert on your credit reports, and review your credit reports.**
   Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You need to contact only one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

   - **Equifax:** 1-800-525-6285;
     www.equifax.com;
     P.O. Box 740241, Atlanta, GA 30374-0241

   - **Experian:** 1-888-EXPERIAN (397-3742);
     www.experian.com;
     P.O. Box 9532, Allen, TX 75013

- **TransUnion:** 1-800-680-7289;
  www.transunion.com;
  Fraud Victim Assistance Division,
  P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information like your SSN, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, contact the consumer reporting companies to get it removed. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

FRAUD ALERTS

- **An initial alert stays on your credit report for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or could be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies.
- **An extended alert stays on your credit report for seven years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report" (see page 20). When you place an extended alert on your credit report, you're entitled to two free credit reports within 12 months from each of the three nationwide consumer reporting companies.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your SSN, name, address, and other personal information requested by the consumer reporting company.

When a business sees the alert on your credit report, they must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

THE IDENTITY THEFT REPORT

An identity theft report may have two parts:

Part One is a copy of a report filed with a local, state, or federal law enforcement agency, like your local police department, your state Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. When you file a report, provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened, and the alleged identity thief.

Part Two of an identity theft report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the consumer reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your identity theft report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your identity theft report as incomplete. You will have to resubmit your identity theft report with the correct information.

2. **Close the accounts that you know, or believe, have been tampered with or opened fraudulently.**
   Call and speak to someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. *It's important to notify credit card companies and banks in writing.* Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

   When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. 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.

   If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.

   - For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, write a letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

- For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit. If not, ask the representative to send you the company's fraud dispute forms. If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information.

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.

3. **File a report with your local police or the police in the community where the identity theft took place.**
   Then, get a copy of the police report, or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check **www.naag.org** for a list of state Attorneys General.

4. **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.

   You can file a complaint online at **www.consumer.gov/idtheft**. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Be sure to call the Hotline to update your complaint if you have any additional information or problems.

FOR MORE INFORMATION

The FTC publishes a series of publications about the importance of personal information privacy. To request free copies of brochures, visit **ftc.gov** or call 1-877-FTC-HELP (382-4357).

Avoiding Credit and Charge Card Fraud

Credit Card Loss Protection Offers: They're The Real Steal

Credit, Debit and ATM Cards: What To Do If They're Lost or Stolen

Electronic Banking

Fair Credit Billing

Fair Debt Collection

File-Sharing: A Fair Share? Maybe Not

How Not to Get Hooked by a 'Phishing' Scam

How to Dispute Credit Report Errors

Site-Seeing on the Internet: A Traveler's Guide to Cyberspace

Spyware

Your Access to Free Credit Reports

PRIVACY POLICY

When you contact the FTC with complaints or requests for information, you can do it online at **www.consumer.gov/idtheft**; by telephone, toll free at 1-877-ID-THEFT (438-4338); or by mail: Federal Trade Commission, Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

The information you send is entered into the Identity Theft Clearinghouse, an electronic database. The Clearinghouse is a system of records covered under the Privacy Act of 1974. In general, the Privacy Act prohibits unauthorized disclosures of the records it protects. It also gives individuals the right to review records about themselves. Learn more about your Privacy Act rights and the FTC's Privacy Act procedures by contacting the FTC's Freedom of Information Act Office: 202-326-2430; **ftc.gov/foia/privacy_act.htm**.

The information you submit is shared with FTC attorneys and investigators. It also may be shared with employees of various federal, state, or local law enforcement or regulatory authorities, and with some private entities, such as consumer reporting companies and any companies you may have complained about, when it believes 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 some circumstances, including requests from Congress, the FTC 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 agencies and other organizations will not be able to contact you for more information to help in identity theft investigations and prosecutions.