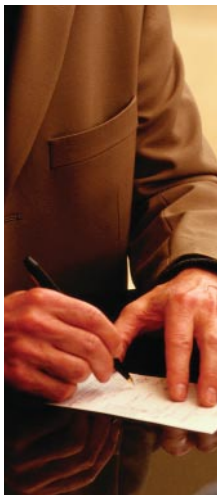
PROTECT YOUR IDENTITY

Tips and Tools for Safeguarding
Your Personal Information
From Being Used Fraudulently

VISA



What Is ID Theft?

Identity theft is one of the fastest growing crimes in the United States today. Recent statistics show that each year approximately 700,000 individuals are falling victim to a new breed of criminal known as "identity thieves." These crooks are out there in both the physical and virtual worlds, looking around for valuable pieces of personal information that belong to someone else.

For the identity thief, the phrase "a little goes a long way" rings true. With a minimal amount of valid information (e.g., Social Security number, driver's license, etc.), a skilled thief can quickly assume an individual's identity to conduct numerous crimes such as:

- ✔ opening new bank accounts and writing bad checks
- ✔ establishing new credit card accounts and not paying the bills
- ✔ obtaining personal or car loans
- ✔ getting cash advances
- ✔ establishing a cellular phone or utility service and running up bills
- ✔ changing your credit card mailing address and charging on your existing accounts
- ✔ obtaining employment
- ✔ renting an apartment, then avoiding the rent payments and getting evicted

What Do Victims Face?

One of the biggest problems with cases involving identity theft is that it can take months before the victim is aware of any wrongdoing. The victim typically learns of the crime after he or she receives a collection agency letter or is turned down for a loan because of a negative credit rating. When it gets to this point, a victim will often end up spending many hours reclaiming his or her identity and straightening out financial matters.

How Does Someone Steal an Identity?

ID theft can occur in a number of different ways. Here are some common scenarios.

- **Dumpster Diving –** Thieves rummage through trash cans searching for pieces of unshredded personal information that they can use or sell.

- **Mail Theft –** Crooks seek out and steal from unattended/unlocked mailboxes to obtain pre-approved credit offers, bank statements, tax forms, and/or convenience checks. They also look for credit card payment envelopes that have been left in the mailbox for postal carrier pick-up.

- **Inside Sources –** A dishonest employee with access to personnel records, payroll information, insurance files, account numbers and/or sales records can wreak havoc.

- **Imposters –** Many identity theft victims have been taken in by an individual who fraudulently posed as someone who had a legitimate or legal reason to access the victim's personal information (e.g., landlord asking for background information, an employer, marketer, etc.).

- **Online Data –** On the simplest level, thieves access data that consumers share through phone listings, directories, memberships, etc. Thieves can also purchase sensitive personal information about someone (e.g., name, address, phone numbers, Social Security number, birth date, etc.) from an online broker.

- **Direct Access to Personal Documents in the Home –** Unfortunately, there are identity thieves who can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends or roommates, etc.

- **Purse/Wallet Theft –** Stolen purses and wallets usually contain plenty of bankcards and personal identification. A thief can have a field day using this information to obtain credit under the victim's name or sell the information to an organized-crime ring.

What Should I Do If I Become a Victim of Identity Theft?

1 Contact the three national credit bureaus to:

- Report the identity theft and request a "fraud alert." This ensures that you will be contacted before any new account is opened and/or an existing account is changed.
- Request copies of credit reports. Review the reports carefully and identify any new accounts that may have been opened. Pay particular attention to the section of the report that lists "inquiries" from new companies. Contact these companies immediately and have them remove any pending or new accounts from their system.

CREDIT BUREAU	CONTACT DETAILS
Equifax www.equifax.com	800-525-6285 (Fraud Hotline) 800-685-1111 (Report Order)
Experian www.experian.com	888-397-3742 (Fraud Hotline) 888-397-3742 (Report Order)
TransUnion www.transunion.com	800-680-7289 (Fraud Hotline) 800-916-8800 (Report Order)

CREDIT BUREAUS MUST PROVIDE FREE COPIES OF CREDIT REPORTS TO VICTIMS OF IDENTITY THEFT.

2 File a police report.

Get a report number and/or copy of the report should anyone request proof of the crime.

3 Contact the fraud departments of creditors

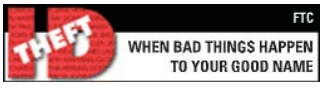
(e.g., credit card issuers, phone companies, utilities, banks, other lenders, etc.). Describe your identity theft problem and follow up with a letter or affidavit. This is very important for credit card issuers, since the consumer protection law requires cardholders to submit disputes in writing.

4 File a complaint with the Federal Trade Commission (FTC).

The FTC handles complaints from victims of identity theft, provides information to those victims, and refers complaints to appropriate entities, including the major credit-reporting agencies and law enforcement agencies.

FTC CONTACT DETAILS	
BY PHONE	*USING ONLINE COMPLAINT FORM*
Toll-free 1-877-ID-THEFT (1-877-438-4338); **TDD:** 202-326-2502	www.consumer.gov/idtheft

The ID Theft Affidavit is a special tool developed to help simplify the ID theft reporting process for consumers. It is a standard form that can be used by victims to report the same information to different companies, such as the three major credit bureaus, and other banks or creditors where an account has been opened and/or used under the victim's name.



For a copy of the ID Theft Affidavit, visit www.consumer.gov/idtheft or call 1-877-ID-THEFT.

5 Take appropriate actions, depending on your identity theft circumstances:

IF YOU SUSPECT:	DO THE FOLLOWING:
✔ your mail has been stolen to obtain bank and credit card statements, bills, pre-screened credit offers, etc., or the thief has submitted a change-of-address form to redirect mail	File a report with the U.S. Postal Inspection Service Office. Telephone numbers are listed in the white pages under federal government.
✔ the thief has changed a billing address on a credit card account	• Contact your credit card-issuing bank to establish a password to be used before any inquiries or changes are made on the account. • Close all accounts that have been tampered with; request new PINs and passwords.
✔ your Social Security number (SSN) has been stolen	Contact the nearest Social Security Administration office to report the suspected abuse.

Am I Liable for Unauthorized Visa Card Charges Made Under My Name?

$0 Visa offers consumers zero liability* fraud protection for unauthorized transactions. If you discover unauthorized Visa credit or check card charges under your name, your liability is $0—you pay nothing.

**U.S.-issued only. The Zero Liability policy does not apply to commercial card or ATM transactions, or to PIN transactions not processed by Visa. See your Cardholder Agreement for more details.*

Under the Fair Credit Billing Act, consumer liability for unauthorized credit cards is limited; in most cases, to $50 per card.

Where Can I Find Out More About ID Theft?

The Internet is full of Web sites offering helpful advice on ID theft. To access publications on the subject and find out more about what you can do to protect yourself, check out these sites:

Call for Action	www.callforaction.org
Federal Trade Commission	www.consumer.gov/idtheft
Social Security Administration	www.ssa.gov
U.S. Postal Inspection Service	www.usps.gov/postalinspectors

What Can I Do to Guard Against Identity Theft?

There are several actions you can take to protect your personal information and minimize risk of identity theft.

DO…

- ✔ Shred all personal and financial information (e.g., bank statements, credit/ATM receipts, credit card offers, credit card bills, etc.) before you throw it away.
- ✔ Keep your personal (e.g. Social Security card, birth certificate, etc.) and bank/credit card records in a secure place.
- ✔ Call the post office immediately if you are not receiving your mail. Some crooks are able to forge your signature and have your mail forwarded elsewhere for the purpose of obtaining information that will allow them to apply for credit in your name.
- ✔ Be aware of others nearby when entering your Personal Identification Number (PIN) at an ATM.
- ✔ Limit the number of credit cards and other personal information that you carry in your wallet or purse.
- ✔ Report lost or stolen credit cards immediately.
- ✔ Cancel all inactive credit card accounts. Even though you do not use them, those accounts appear on your credit report, which can be used by thieves.
- ✔ If you have applied for a credit card and have not received the card in a timely manner, immediately notify the financial institution involved.
- ✔ Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to the expiration date on your credit card.
- ✔ Sign all new credit cards upon receipt.
- ✔ Review your credit reports annually to safeguard your identity.
- ✔ Use passwords on your credit cards, bank accounts, and phone cards. (Avoid using the standard mother's maiden name, birth date, and the last four digits of your Social Security or phone number.)
- ✔ Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.
- ✔ If your Social Security number is being used for identification purposes (e.g. health insurance, doctor's office), request another method of identification.

DON'T…

- ✔ Volunteer any personal information when you use your credit card.
- ✔ Give your Social Security number, credit card number, or any bank account details over the phone unless you have initiated the call and know the business that you are dealing with is reputable.
- ✔ Leave receipts at ATMs, bank counters, or unattended gasoline pumps.
- ✔ Leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.
- ✔ Record your Social Security number and/or passwords on paper and store them in your wallet or purse. Memorize your numbers and/or passwords.
- ✔ Disclose bank account numbers, credit card account numbers, and other personal financial data on any Web site or online service location, unless you receive a secured authentication key from your provider.

VISA