

# Identity Theft

(BOOKMARKS to different sections on page.)

- [How to Protect Your Personal Information](#)
- [10 Steps to Recover from ID Theft](#)
- [ID Theft Passport](#)
- [Sample Dispute Letters](#)
- [Contact](#)

DRAFT

## Additional Resources

- Federal Trade Commission
  - [ID Theft](#)
  - [Free Annual Credit Reports](#)
  - [Phishing Scams](#)

**Identity theft** is now the top-reported form of crime in the United States. This crime occurs when someone acquires key pieces of another person's identifying information – such as his name, Social Security Number, date of birth and financial information – in order to impersonate that person. The thief may use this information to:

- take over a victim's financial accounts or open new credit accounts in the victim's name to run up charges
- establish phone or wireless service in the victim's name
- open bank accounts in the victim's name and writing bad checks
- get loans in the victim's name and never repay them, ruining the victim's credit rating
- rent apartments or buy cars in the victim's name
- use the victim's name when committing crimes or driving offenses, resulting in warrants being issued in the victim's name

Identity theft can happen to anyone. Each of us is a potential victim.

Identity thieves steal information:

DRAFT

- **From the trash.** Identity thieves get copies of credit card receipts, credit applications and other information that have been placed in trash containers.
- **From the mailbox.** Thieves steal letters waiting to be picked up by postal carriers.
- **From stolen wallets or purses.**
- **By using email.** Thieves often pose as legitimate companies someone does business with in order to obtain personal information.
- **By using the Internet.** Internet abusers can steal information people share on the Internet or piece together information available about someone on the Internet.
- **From employee records.** Dishonest personnel can access employee or other personal records and sell this information to identity thieves.

## How to Protect Your Personal Information

There are a number of important steps people can take to better protect themselves:

- **Never give bank or credit card information** o' the call and know the business to be reputable.

Economic Affairs Committee Meeting  
October 28, 2005

Exhibit #12

- **Never respond to e-mail or pop-up messages** asking you to confirm or verify account information, even if it looks official. Instead, call the customer service number listed on the company's billing statement to check an account.
- **Remove extra information from your checks.** Merchants cannot require you to write your social security number, date of birth or phone number on a check.
- **Shred or destroy any documents** that contain personal identifying information before you dispose of them. Always shred prescriptions, receipts, bank deposit slips, pay stubs, expired credit cards, insurance policies and credit card applications.
- **Opt out of pre-screened credit card offers** by calling 1-888-5-OPTOUT (567-8688).
- **Review your bank and credit card statements** as soon as you get them.
- **Order a copy of your credit report** once a year and check it carefully for fraudulent accounts. You are entitled to a free copy once every 12 months.
- **Read and understand privacy and security policies** before providing any personal information on Internet sites. Shop online only if the site is secure.
- **Place passwords on your credit card, bank and phone accounts** and avoid using easily available information such as your mother's maiden name.
- **Secure personal information** in your home.

DRAFT

## 10 Steps to Recover from Identity Theft

- **10 Steps Bookmark**

Victims of identity theft must act quickly to minimize the damage. The following information is provided to assist individuals who are or suspect they may be victims of identity theft. It is intended as a general guide, not as legal advice.

1. **Keep a record of whom you call and when.** It is very important to keep good notes of all conversations and records of all correspondence with your financial institutions and law enforcement agencies, including a log of the names, dates and phone number of people you contacted. You also should confirm the information in writing. Sending your letters by certified mail, return receipt requested, provides you with a record of your correspondence.
2. **Contact the fraud departments of the three major credit bureaus.** Ask that they put a "fraud alert" on your account and send you a free credit report:

DRAFT

Credit Bureau	Mailing Address	Phone Number	Website Address
<b>Equifax</b>	P.O. Box 740241 Atlanta, GA 30374-0241	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
<b>Experian</b>	P.O. Box 9532 Allen, TX 75013	1-888-EXPERIAN (397-3742)	<a href="http://www.experian.com">www.experian.com</a>
<b>TransUnion</b> Fraud Victim Assistance Division	P.O. Box 6790 Fullerton, CA 92834-6790	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

3. **Report the theft of your identity to your local law enforcement agency.** Ask for a copy of the police report, and to have your case entered into the NCIC Identity Theft File. Credit card companies and financial institutions may require you to show a copy of this report to verify the crime. Keep the phone number of your investigator and provide it to creditors and others who require verification of your case.

4. **Complete an Identity Theft Passport application** and return it to the law enforcement agency you reported the crime to in Step 3. Remember to include a copy of your driver's license. Law enforcement will send the completed form to the Identity Theft Passport Program.

5. **Report the crime to the Federal Trade Commission and complete an FTC ID Fraud Affidavit.** Don't mail it to the FTC – see Step 6.

**Federal Trade Commission**

Phone: 1-877-IDTHEFT (438-4338) or TTY: 1-866-653-4261

Website: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

6. **Mail copies of the following to all three credit bureaus** and to all creditors and collection agencies showing or collecting the fraudulent charges:

- the FTC ID Fraud Affidavit
- the police report
- your Identity Theft Passport (if you have one), and
- a letter disputing the fraudulent charges.

**DRAFT**

The dispute letter **must do all** of the following:

- identify you
- indicate which accounts are disputed
- affirmatively state that you had nothing to do with the charges on the accounts
- request that the accounts be blocked from your credit report

Sample dispute letters are available for:

- [existing credit accounts \(Link\)](#)
- [credit bureaus\(Link\)](#)

7. **Notify all financial institutions** you have an account with that you are a victim of identity theft. Change your account numbers and passwords. (For any accounts that have been fraudulently accessed or opened, contact the billing inquiries and security departments of the appropriate creditors or financial institutions. Close these accounts. Use passwords - not your mother's maiden name - on any new accounts opened. Confirm your contact in writing. Ask that old accounts be processed as "account closed at consumer's request," not "card lost or stolen." When the latter is reported to credit bureaus, it can be interpreted as blaming you for the loss. Carefully monitor your mail and credit card bills and immediately report any new fraudulent activity to credit grantors.)

**DRAFT**

8. **Request a copy of your federal criminal history report.** The application is available online or from the ID Theft Passport Program, 1-406-444-3728.

**FBI Criminal History Report**

[www.fbi.gov/hq/cjisd/fprequest.htm](http://www.fbi.gov/hq/cjisd/fprequest.htm)

9. **Check your credit report with all three credit bureaus** (listed in Step 2) at least every three months until the matter is resolved.

10. Pay any portion of a bill that is legitimate, but **DO NOT pay charges you are disputing.** (Your credit rating should not be permanently affected, and no legal action

should be taken against you as a result of identity theft. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.)

## **Identity Theft Passport Program**

**DRAFT**

- Passport Application

In October 2005, the Attorney General's Office instituted a new Identity Theft Passport program. The passport is intended to help victims prove to creditors and law enforcement officers that someone has used their identity to commit fraud.

Through no fault of their own, victims of identity theft are forced to spend a considerable amount of time and money undoing the damage done to their good names and credit records. The wallet-sized passport is designed to help victims prove who they are and limit the cost and stress they experience.

To qualify for a passport, identity theft victims must file a police report and present a completed Identity Theft Passport application to the investigating agency. Once the complaint has been verified by law enforcement, the agency faxes or mails to Montana's Office of Consumer Protection and Victim Services:

- a copy of the completed investigation report
- the Identity Theft Passport application, signed by the victim and the officer
- a copy of the victim's driver license or other official form of photo identification

The passport application and supporting documentation is confidential criminal justice information. Law enforcement agencies and creditors have discretion in accepting an identity theft passport. The passport simply indicates that the agency or company should take into consideration that the individual is a victim of identity theft.

## **Contact the Office of Consumer Protection and Victim Services**

### **Passport Program**

Michelle Truax  
1712 9th Avenue  
PO Box 201410  
Helena, MT 59620-1410

Phone: (406) 444-3728  
E-mail: [mitruax@mt.gov](mailto:mitruax@mt.gov)  
Fax: (406) 444-4303

**DRAFT**