Identity Theft Handbook

Steps to Protect Yourself
What to Do If You Are a Victim
Policies to Reduce Identity Theft

MaryPIRG Foundation

What Is Identity Theft?

Identity theft is the crime of stealing an individual's personal identifying information for the purpose of committing fraud or theft. The most common types of identity theft are using a credit card to make purchases, withdrawing money from a person's bank account, and signing up for phone service or other utilities in someone's name. Many other cases involve taking out a loan from a bank or other institution in someone else's name. Some cases involve posing as someone else when caught committing a crime.

The Crime of the New Millennium

Identity theft is the fastest growing crime in America. A recent survey by the Federal Trade Commission found that one in ten Americans was a victim of identity theft within the past five years. During 2003, over half a million Americans filed complaints of consumer fraud and identity theft with the FTC. Approximately 42 percent of all complaints filed were in regard to identity theft.

Costs to Consumers

Fraud costs consumers almost half a billion dollars annually. The average consumer spends 175 hours and $808 "out-of-pocket" to remedy identity theft. In total, this crime drains the economy of over $50 billion annually, and some of that cost is borne directly by consumers.

Even if the theft is discovered, consumers may continue to experience negative effects, such as increased insurance or credit card fees, higher interest rates, and persistent collection agencies that refuse to clear false records. Furthermore, the emotional and psychological impact suffered by identity theft victims cannot be understated. They must struggle for months or even years to restore their good name.

In 2003, over 4,000 Marylanders were defrauded an average of $1,900.

Maryland: Hit Hard

Marylanders are no strangers to identity theft. The Washington metropolitan area had the highest per capita rate of identity theft complaints in the country in 2003, and Baltimore had the 10th highest.

In 2003, over 4,000 Marylanders were defrauded an average of $1,900.

How Do I Reduce My Risk of Identity Theft?

Despite the prevalence of identity theft, you can reduce your risk of becoming a victim through common sense measures and taking some precautionary steps. Companies marketing fraud protection programs are often charging for things they should be doing anyway or offering services you can get yourself for free. We recommend simply being aware of your risks and following the steps outlined in this handbook. You'll never be risk-free, but you can reduce your risk significantly.

Credit Reports

Check your credit report annually with the three major national credit bureaus, Equifax, Experian, and TransUnion, to make sure your accounts are not being misused and that no unauthorized accounts have been opened in your name. You can also check your credit report for mistakes not attributable to identity theft that may nevertheless damage your credit rating.

Equifax: (800) 685-1111 or www.equifax.com
Experian: (888) 397-3742 or www.experian.com/freestate
TransUnion: (800) 888-4213 or www.transunion.com

Since 1992, Maryland residents have had the right to obtain one free credit report annually from each of the major credit bureaus. By September 1, 2005, Marylanders will be able to obtain their free annual credit reports from each bureau through a centralized source, rather than contacting each bureau separately.

Your Social Security Number

- **Limit exposure of your Social Security number** by giving it only when it is absolutely necessary.
- **Do not** allow banks, health insurance companies or other institutions to print your SSN on common items such as personal checks and ID cards.
- If a business requests your SSN for check cashing purposes, ask to **use another type of identifying information**.

Using Your Personal Identifying Information

Do not give bank account numbers or other personal information, over the phone, through the mail, or on the Internet to individuals or businesses, unless you have initiated the contact or are certain of the business' trustworthiness.

Before you give your personal identifying information, ask how the information will be used, how the business will protect your information from theft, and how your personal information will be destroyed when the business no longer needs it.

Your Social Security number is the main key into your credit line.

Credit Cards

- **Limit** the number of credit cards you carry on a daily basis.
- **Keep a list** of your credit card and bank accounts in a secure place that can be easily accessed in case you are a victim of theft. Include account numbers, expiration dates, and telephone numbers of customer service and fraud departments. Do not carry this list in your wallet.
- **Follow up.** If you are expecting a new or reissued credit card, contact the issuer if the card does not arrive when you expect it.
- **Cancel inactive credit cards.** If you no longer receive monthly statements because you have not used a card recently, you may not notice unusual or fraudulent activity until it is too late.

Debit Cards

Although debit cards may be more convenient than other types of payment, consumers should be cautious when using them.

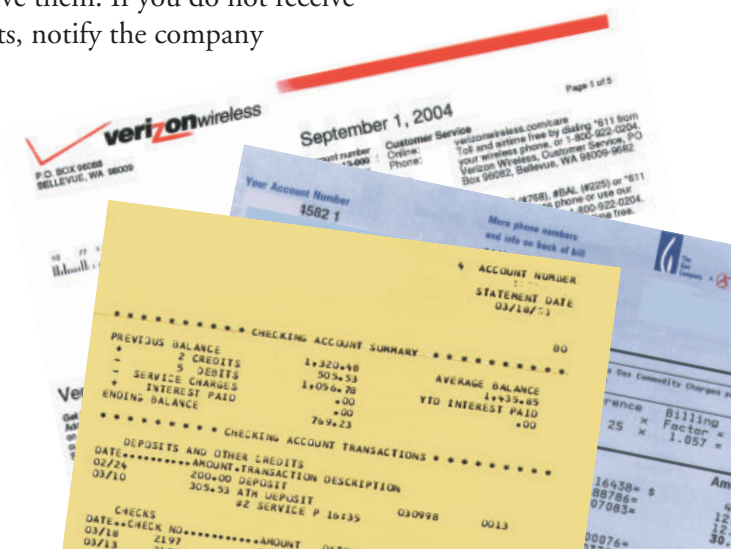
Debit cards are riskier than traditional ATM cards or credit cards. While you are only liable for $50 if your credit card is used fraudulently, you may be liable for $500 or more if your debit card is misused. Furthermore, laws regulating credit cards offer consumers protection if the goods they order are defective or don't arrive; these protections aren't available if you use a debit card.

- **It is best not to use a debit card at all.** You can tell your bank not to issue a debit card for your account.
- If you do use a debit card, **make sure you always keep it in your possession.** If your ATM or debit card has been stolen or misused, report it immediately to your bank branch and request a fraud affidavit. Obtain a new card, account number, and password.

Debit cards have high liability and little consumer protection.

Keeping Track of Financial Accounts

- **Reconcile** your check, credit card, and other account statements on a regular basis and notify businesses or banks of any mistakes.
- **Review** your utility and subscription bills to make sure any charges are yours.
- **Make a list** of your bills and the approximate time of month you receive them. If you do not receive billing statements, notify the company immediately.



Online

In recent years, identity thieves have increasingly been using the Internet to perpetrate their crimes. In 2003, 55 percent of consumer fraud complaints reported to the FTC were Internet-related, accounting for $200 million in losses.

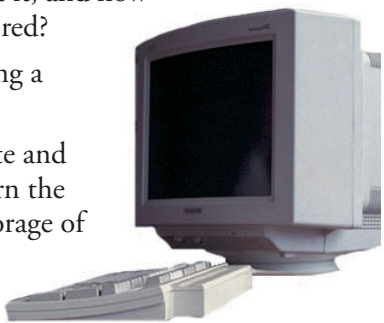
There are several steps you can take to protect yourself.

- **Do not download or open files from strangers**; opening a file could expose your computer system to a virus that allows strangers to access your personal information.
- **Use a "firewall"** for high-speed Internet connections, and **use a secure browser** that encrypts, or scrambles, information you send over the Internet.
- If you are making purchases online, **use a credit card, not a debit card**. Credit cards provide more consumer protection and less liability in the event of theft.

In 2003, 55% of consumer fraud complaints reported to the FTC were Internet-related.

If you are going to transmit personal information through a website, read the site's privacy policy. Secure websites will have a locked padlock at the bottom right on the browser status line or *https://* (with an "s") in the address line instead of *http://*. A website's privacy policy should answer the following:

- How and why is personal information being collected?
- How is the information used? Is it for a purpose other than that for which it was provided?
- Is encryption used when transmitting information?
- Do you have the option of prohibiting any secondary use or of not providing any personal information?
- If you must provide personal information, can you access and correct it, and how long will it be stored?
- How can you bring a complaint?
- What specific state and federal laws govern the collection and storage of information?



"Phishing"— A New Scam

Beware of a new type of scam known as "phishing." In these scenarios, **thieves set up web sites that look like the sites of legitimate businesses**. They trick consumers into entering their personal information by sending them e-mail messages that claim there is a problem with their account.

If you get an e-mail message requesting your account information or other personal information, you should call the business at its published phone number or log onto the business' website by typing in the website address, not by clicking a link.

Solicitations

An effective way to protect yourself from fraud, and to reduce the amount of junk mail you receive, is to **opt out of junk mail.** If it is not discarded properly, junk mail can be a source of personal information for thieves.

To stop receiving pre-approved credit or insurance solicitations derived from credit reports, you can "opt out" for two years or permanently. **Call the Federal Trade Commission at (888) 567-8688.** To opt out permanently, you must choose "option 2" when you call and sign a notice of election sent through the mail.

To discontinue non-credit offers generated by lists kept by the major credit bureaus, write to each.

Experian: Consumer Opt-Out
701 Experian Parkway, Allen, TX 75013

Equifax: Options
P.O. Box 740123, Atlanta, GA 30374

TransUnion: Marketing List Opt Out
P.O. Box 97328, Jackson, MS 39288

To be removed from mail, e-mail, and telephone marketing lists, visit the **Direct Marketing Association website:** www.dmaconsumers.org.

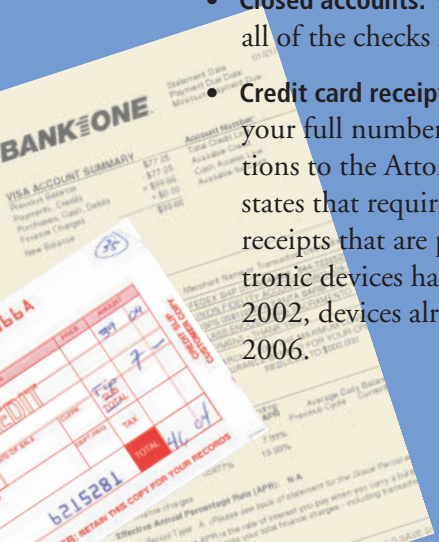
Federal Do-Not-Call List
888-382-1222 (TTY 866-290-4236)
www.donotcall.gov

Mail

- **To protect your mail, install a lockable mailbox.**
- **If you are going on vacation, have your mail held at your local Post Office, or picked up by a person you trust.**
- **Put your outgoing mail in a United States Postal Service mailbox, rather than leaving it for the postal carrier to pick up.**

Personal Documents

- **Receipts.** After making transactions at an ATM or business, take your credit card, debit card, and ATM receipts. Do not dispose of these receipts or any documents with personal identifying information in public receptacles. "Dumpster divers" may use your information to order credit cards or gain access to your bank account.
- **New checks.** When you order new personal checks, pick them up at the bank rather than having them sent to your home.
- **Closed accounts.** When you close a checking account, destroy all of the checks immediately.
- **Credit card receipts.** Be careful with receipts that still have your full number on them, and report any suspected violations to the Attorney General. Maryland is one of twenty states that requires truncation of credit card numbers on receipts that are printed electronically. Although new electronic devices had to comply with this law as of October 1, 2002, devices already in use need not comply until January 1, 2006.



Theft of business records

Identity Theft in the Workplace

Theft of business records is the number one source of identity theft according to a 2002 report by the credit bureau TransUnion. The FTC reports that 90 percent of business record theft involves stealing payroll or employment records. In addition, there are reported cases of thieves obtaining employment in small businesses such as doctors' offices to gain access to, or "harvest," patient or customer records.

Employees should ask **what policies are in place** to protect their personal information. Privacy policies should:

- Prohibit the use of SSNs as an identifier.
- Restrict access to employees' and customers' personal information.
- Detail basic security precautions, such as locking storage areas where sensitive information is kept, using passwords to access personal information, and training employees who handle sensitive information.
- Guard against identity theft by employees of third-party vendors, like temporary or contract workers.
- Require destruction of personal information once it is no longer needed.

is the number one source of identity theft.

What Do I Do if I Am a Victim?

You may be a victim of identity theft if you:

- Fail to receive bills or other mail, signaling a change of address by the thief.
- Receive credit cards that you did not apply for.
- Are denied credit for no apparent reason.
- Receive calls from debt collectors or companies in reference to debts you do not owe or merchandise or services you did not purchase.

Four Important Steps

In general, if you suspect you are a victim of identity theft or fraud you should not be responsible for fraudulent charges, but you do need to clear your name. To lessen the impact of fraud and theft, take the following steps immediately:

1. **Contact one of the three major credit bureaus.**
   Place a fraud alert on your credit report and obtain free credit reports. Once your alert has been confirmed by the bureau, the other two bureaus will be notified and all three must send you a free credit report. Fraud victims are entitled to a free report from each bureau, even if they have already obtained one under their state's law.

2. **Remove accounts from your credit report that aren't yours.**
   Ask companies to close any accounts that have been opened fraudulently. Close any of your accounts that have been tampered with.

3. File a report with local police.

Over half of consumer fraud and identity theft is never reported to law enforcement. However, police may be able to recover stolen money and prevent further crime. In some instances, you won't qualify for legal protection unless you have filed a police report.

4. File complaints with government agencies.

Federal Trade Commission
Identity Theft Hotline
877-IDTHEFT / 877-438-4338

Maryland Commissioner
of Financial Regulation
410-230-6100

Maryland Attorney General's
Consumer Protection Division
410-528-8662

Keep careful records of all communications about your case.

Stolen checks or fraudulent bank accounts

If you suspect one of your checks has been stolen, close the account and request the bank to notify the appropriate check verification company.

If you know that a particular merchant has received a stolen check in your name, contact the verification company used by that merchant.

Credit cards

If a new credit account has been set up in your name, contact the creditors immediately by phone and in writing. Most creditors will allow you to use the fraud affidavit provided by the FTC (www.consumer.gov/idtheft).

If your existing credit account has been used fraudulently, get a replacement card with a new number. Request your old account be processed as "account closed at consumer's request."

Debt Collectors

If debt collectors attempt to collect on fraudulent accounts, take the following steps:

- Tell them that you are a victim of fraud and are not responsible for the account.
- Record the collecting agency's name, contact information, and the name of the person who contacted you.
- Get the name and contact information of the referring credit issuer, the amount of the debt, the account number, and the dates of the charges.
- Ask if they need you to complete a fraud affidavit.
- Follow up in writing with the debt collector and request that they confirm in writing that you are not responsible for the debt and that the account has been closed.

Additional Resources

Social Security fraud, contact the Social Security Administration: 800-269-0271

Tax fraud or violations, contact the Internal Revenue Service: 800-829-0433

Fraudulent use of the **mail system** or submission of fraudulent change-of-address form, contact the U.S. Postal Inspection Service: 202-636-2300

You can also call your local office of the FBI or the U.S. Secret Service to report crimes relating to identity theft and fraud. The Secret Service can handle financial fraud, but it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring:

Baltimore FBI Field Office: 410-265-8080

Maryland Secret Service Field Office: 443-263-1000

Resources (continued)

To locate a **lawyer** who specializes in consumer law, contact a local **Legal Referral Service**.

Baltimore City: 410-539-3112
Baltimore County: 410-337-9100
Anne Arundel County: 410-280-6961
Montgomery County: 301-279-9100
Howard County: 410-465-2721
Maryland Legal Assistance Network: 410-576-9494
Maryland Trial Lawyers Association: 410-246-2292

Your Costs

Document the time and money you spend remedying the theft. In some states, individuals found guilty of identity theft may be ordered to pay restitution for financial losses, such as lost wages and lost time. If the thief is caught, you can write a victim impact letter to be used in the case.

What Policies Do We Need to Decrease Identity Theft

Maryland residents have some protection against identity theft under state and federal law, but more protections are needed.

The State of Maryland should take the following steps immediately.

1. **Use of Social Security Numbers**

   State law should prohibit the public display of Social Security numbers, including the printing of SSNs on ID cards or account notices.

2. **Anti-Coercion Laws**

   Anti-coercion laws should prohibit companies from refusing to serve customers who do not want to provide their SSN or other personal information. Companies should not be allowed to require an individual's SSN to access an Internet website.

3. **Police Reports**

   Police reports are often required by credit bureaus to expunge the record of victims of identity theft. These reports are also required in order to get an extended fraud alert and to access business records to document fraud. Unfortunately, it is sometimes difficult to get law enforcement agencies to take a report. Police should be required to take a report when investigating identity theft so that victims can clear their credit records.

   Also, the Maryland Attorney General should have the authority as a law enforcement agency to take a police report or an FTC identity theft affidavit.

4. Factual Declaration of Innocence

Victims of identity theft are allowed to petition the court for a "factual declaration of innocence." The state would issue the victim an official record of that declaration, and should also establish a database that would keep these records. If the victim loses the paper, this database would contain the order and a copy of the true person's fingerprints for comparison in the case of another mistaken identity.

5. Criminal Proceedings

Victims may not only be unaware that their credit has been compromised; they may not know when criminal proceedings regarding the fraud are being held. Laws should require victims to be notified of all steps of the criminal process, including the trial date and the release of the perpetrator from custody. Provisions should also be made to allow for victim input prior to sentencing and for restitution when appropriate.

6. Accuracy Audits

To ensure accuracy and privacy, the Maryland Attorney General should have the same authority as the FTC to receive detailed annual reports from the major credit bureaus regarding their databases and to make a summary of such results available to the public.

7. Sharing Personal Information

Although federal law prohibits credit bureaus from transmitting personal information for marketing purposes, current law does not regulate the bureaus' affiliates. Maryland residents should be able to prohibit credit bureau affiliates from transmitting personal information to businesses for marketing purposes if consumers provide written notification to the credit bureau.

8. Security Freeze

Maryland residents should be able to "freeze" their credit reports for a certain period of time by providing written notice to credit bureaus. When an account is frozen, no credit report may be issued, except to existing creditors or

for insurance or employment purposes, unless permission is granted by the consumer. If a request is made on a "frozen" account, the consumer in question will be notified by the credit reporting agency of the request.

9. Hacker Notification

Consumers should be notified when businesses or government agencies experience a computer security breach of sensitive information, such as SSNs, driver's license numbers, or credit or debit card numbers.

10. Destruction of Personal Information

Businesses should be required to make unreadable any documents that contain sensitive information prior to disposal. At least two states (Georgia and California) require businesses, under threat of penalty, to alter or destroy documents containing consumer information before disposing of them. Similar laws should protect employees.

MaryPIRG Foundation
3121 Saint Paul Street, Suite 26
Baltimore, MD 21218

(410) 467-0439
www.marypirg.org

Harriet Eckstein Graphic Design