

**PROTECT
YOURSELF
AGAINST
IDENTITY
THEFT**



JIM PETRO
ATTORNEY GENERAL

STATE OF OHIO

Dear Consumer:

The personal information we carry in our wallets or purses is invaluable to conducting business in today's world. However, in the wrong hands, this information can give a criminal easy access to our property and assets.

It doesn't take much time or effort to protect against identity theft. Prevention is much easier than repairing the damage done by criminals who want to steal your name and credit. The tips in this booklet can help you secure your personal information. It also contains information about what to do if you are the victim of identity theft, or if your personal information or papers are stolen.

Please do not hesitate to contact our office if you have any questions or concerns about how to protect your identity. For updated information about this and many other consumer issues, please visit our office's web site at www.ag.state.oh.us, and follow the consumer links.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Petro", with a long horizontal flourish extending to the right.

Jim Petro

Attorney General

PROTECT YOURSELF AGAINST IDENTITY THEFT

Identity theft (or “true name fraud”) occurs when a criminal obtains and uses a consumer’s personal information such as credit card numbers, bank account numbers, insurance information, and Social Security numbers to purchase goods or services fraudulently. Generally, criminals will do this by opening new accounts in your name, purchasing products, and then leaving you to pay the bill.

In this age of information, criminals can acquire personal information about others much easier than before. Many legitimate businesses share or sell information about their customers without knowing how it will be used or misused. Now more than ever, consumers need to be proactive about protecting their personal information.

Ohio law addresses the growing problem of identity theft. The law, which went into effect August 25, 1999, follows a federal law passed in 1998, making it unlawful for someone to use another person’s identifying information. The federal law also directed the Federal Trade Commission to establish procedures for victims to follow in order to file a complaint and notify the

appropriate law enforcement agencies and credit bureaus.

Ohio's identity theft law makes it a crime to use personal identifying information of another individual with the intent to fraudulently obtain credit, property, or services. It also takes into account computer and Internet technology, and makes it a crime to aid or abet another person in securing this personal identifying information.

**TO CONTACT THE
FEDERAL TRADE
COMMISSION
ABOUT IDENTITY THEFT –
WRITE, CALL, OR VISIT THEIR
INTERNET SITE:**

**FEDERAL TRADE COMMISSION
CONSUMER RESPONSE CENTER
WASHINGTON, D.C. 20580
(877) FTC-HELP (382-4357)
www.ftc.gov**

HOW TO PROTECT YOURSELF FROM IDENTITY THEFT:

- Order a copy of your credit report once a year from each of the three national credit-reporting agencies (Trans Union, Experian, and Equifax) to check for inaccuracies and fraudulent use of your accounts. Monitoring your credit card statements and your credit report are the most important steps you can take to safeguard your credit identity.
 - To order your report from Equifax, call (800) 685-1111, or go to www.equifax.com.
 - To order your report from Experian, call (888) EXPERIAN (397-3742), or go to www.experian.com.
 - To order your report from TransUnion, call (800) 916-8800, or go to www.transunion.com.
- Remove your name from the marketing lists of the three credit-reporting agencies; this will limit the number of pre-screened offers of credit you receive in the mail. To do this, call the Credit Reporting Industry opt-out phone number. The three major credit bureaus use the same toll-free phone numbers for this service: (800) 353-0809 or (888) 567-8688.

- Another way to remove your name, home address, and home telephone number from many mailing and telephone lists is through the Direct Marketing Association. This free service is only available for individuals and “home” addresses (not businesses). You will be removed from the Direct Marketing Association member lists for five years.

To decrease the amount of national nonprofit or commercial mail you receive at home, contact:

- Mail Preference Service
Attention: Dept 9301235
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512

To reduce the amount of unsolicited e-mail you receive, contact:

- Direct Marketing Association
E-mail Preference Service
www.e-mps.org

To receive fewer unsolicited telemarketing calls, you can register for the Direct Marketing Association’s Telephone Preference Service (TPS), which allows you to “opt out” of national telemarketing lists. Contact:

- Telephone Preference Service
Attention: Dept 9301664
Direct Marketing Association
P.O. Box 282
Carmel, NY 10512

Or you can register online for these services at www.the-dma.org.

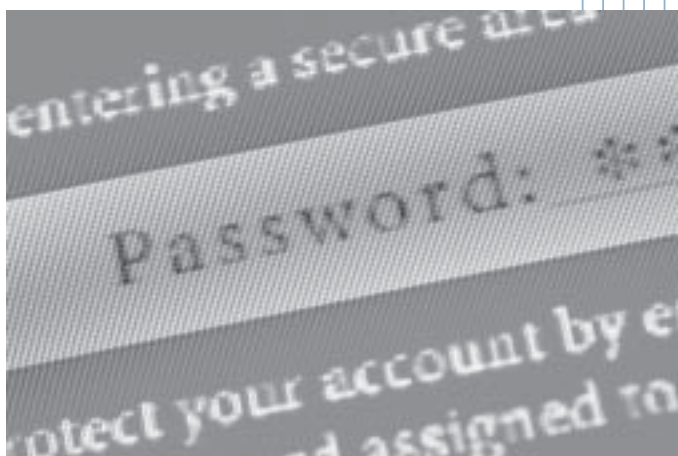
- Do not throw out credit card statements, bills, insurance papers, or bank statements where a criminal could retrieve them from the trash. If you must throw them out, first shred or destroy them.
- When making a credit card purchase from a retailer, ask for credit card carbons if the retailer is not using carbonless forms.
- Reduce the number of credit cards you actively use. Carry only one or two credit cards in your wallet.
- Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded in your credit report, which is full of data that can be used by identity thieves.
- Keep a list or photocopy of all your credit cards, account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a secure place (not in your wallet or purse) so you can quickly contact your creditors in case your cards are lost or stolen. Do the same with your bank accounts.
- Always take credit card and ATM receipts with you. Never toss them in a public trash container.

- Request (in writing) that the issuer for each of your credit cards remove your name from marketing and promotional lists that may be sold or shared with other companies. Also, if any of your credit card issuers send random-issue convenience checks, request (in writing) to be removed from the mailing list. Credit card convenience checks are easy prey for identity thieves to steal and use. Often, the consumer is unaware that the checks were even issued.
- Watch the mail when you are expecting a new credit card. Immediately contact the issuer if the credit card does not arrive.
- Be careful before you use a credit card on the Internet or before providing personal information (such as your Social Security number or date of birth) on an electronic application.
- Never give out personal or financial information over the phone to anyone who calls to solicit a purchase or donation. Before making any transaction, check with your local Better Business Bureau™ or the Attorney General's Office to check the company's business and complaint history.
- Be wary of anyone calling to "confirm" personal or financial information. Often, these are criminals trying to obtain those facts under the guise of "confirmation."

- Thoroughly review your credit card statements, bank statements, utility bills, and insurance bills and statements for any unusual activity, purchases, or charges. Immediately contact the company if an item looks suspicious, or if there is a purchase you don't recall making.

PASSWORDS AND PERSONAL IDENTIFICATION NUMBERS (PINs)

- When creating passwords and PINs, do not use the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, pet's name, address, consecutive numbers, or anything else that could be discovered easily by thieves.
- Ask your financial institution to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use the types of passwords and PINs listed above.



- Memorize all your passwords and PINs. Do not record them on anything in your wallet or purse.
- Shield your hand when using your PIN at a bank ATM or when making long-distance phone calls with your phone card to prevent others from seeing your code.

SOCIAL SECURITY NUMBERS

- Release your Social Security number only when absolutely necessary or when required by law (such as tax forms; employment records; banking, stock, or property transactions; driver's, marriage, or professional license applications; etc.). Your Social Security number is the key to your banking and credit card accounts as well as your insurance and health benefits, making it a prime target of identity thieves.



- Do not carry your Social Security card in your wallet. Keep it at home in a safe and secure place.

- If you think an identity thief is using your Social Security number, call the Social Security Fraud Hotline at (800) 269-0271.

RESPONSIBLE INFORMATION HANDLING

- Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized charges or fraudulent use. Be aware that under current laws, your local telephone company is obliged to let other carriers use its billing system for a fee. More and more unscrupulous third parties are billing consumers for goods such as special services, calling plans, or memberships that they did not order and do not want. Do not agree to any sale or offer over the telephone when the call is unsolicited and you do not know the caller or the company. Ask that promotional materials be mailed to you instead.
- Demand that your financial institution adequately safeguard your personal identifying information. Discourage your bank from using the last four digits of your Social Security number as your assigned PIN. If they have not already done so, request that your bank remove account numbers from ATM receipts. Always take your receipts from ATMs with you and shred or

store them in a safe place. By adopting responsible information handling practices, you and your financial institution can reduce the risk of fraud.

- Avoid paying by credit card if you think the business does not use adequate safeguards to protect your personal information.
- Store your canceled checks in a safe place. In the wrong hands, they could reveal a great deal of infor-



mation about you, including your account number, telephone number, and driver's license number.

- Magazines, credit card companies, clubs, organizations, charities, manufacturers, and retailers make lists of their subscribers, customers, members, and donors available

to other businesses for a fee. Your information is reproduced and sold in countless ways. You should always exercise caution when you are making personal identifying information available. Be careful when using the Internet; sending mail-in rebates, surveys, or warranty cards; entering drawings or sweepstakes; donating money; and even subscribing to magazine services.

IF YOUR PURSE OR WALLET IS STOLEN:

- Immediately file a police report and send copies of the report to your bank, credit card companies, and insurance company.
- Cancel credit card and bank accounts and have new accounts opened with new numbers.
- Report lost or stolen credit cards to the three national credit-reporting agencies in writing (Trans Union, Experian, and Equifax). This is important because if a criminal attempts to fraudulently charge your accounts, you will have established a written record with the credit-reporting agencies of the theft or loss of your cards. You may add a “victim statement” to your records explaining the circumstances under which your cards were lost or stolen. This may protect your credit if fraudulent charges are made to your accounts. You may also ask to be

contacted before any new credit is granted in your name.

IF YOU ARE A VICTIM OF IDENTITY THEFT:

- Immediately contact the police and file a police report. Notify your bank and credit card companies of the fraud. Send copies of the police report to your bank and credit card companies.
- Immediately cancel credit card and bank accounts and have new accounts opened with new numbers.
- Contact the creditors of any accounts that have been tampered with or fraudulently used.
- Contact the fraud department of each of the three national credit bureaus. Add a “fraud alert” to your credit file to aid in the prevention of further fraudulent activities.
 - Experian – To report fraud, call: (888) EXPERIAN (397-3742).
 - Equifax – To report fraud, call: (800) 525-6285.
 - TransUnion – To report fraud, call: (800) 680-7289.

**CONSUMER PROTECTION
SECTION
30 E. BROAD ST., 14TH FL.
COLUMBUS, OHIO 43215-3400**

**THE TOLL-FREE
CONSUMER PROTECTION LINE:
(800) 282-0515**

**FOR TTY USERS, PLEASE CALL
995-7147 (COLUMBUS) OR
(888) 567-6881**

www.ag.state.oh.us



**JIM PETRO
ATTORNEY GENERAL**

STATE OF OHIO



ATTORNEY GENERAL JIM PETRO

**CONSUMER PROTECTION
SECTION
30 E. BROAD ST., 14TH FL.
COLUMBUS, OHIO 43215-3400**

**THE TOLL-FREE
CONSUMER PROTECTION LINE:
(800) 282-0515**

**FOR TTY USERS, PLEASE CALL
995-7147 (COLUMBUS) OR
(888) 567-6881**

www.ag.state.oh.us



**JIM PETRO
ATTORNEY GENERAL**

STATE OF OHIO