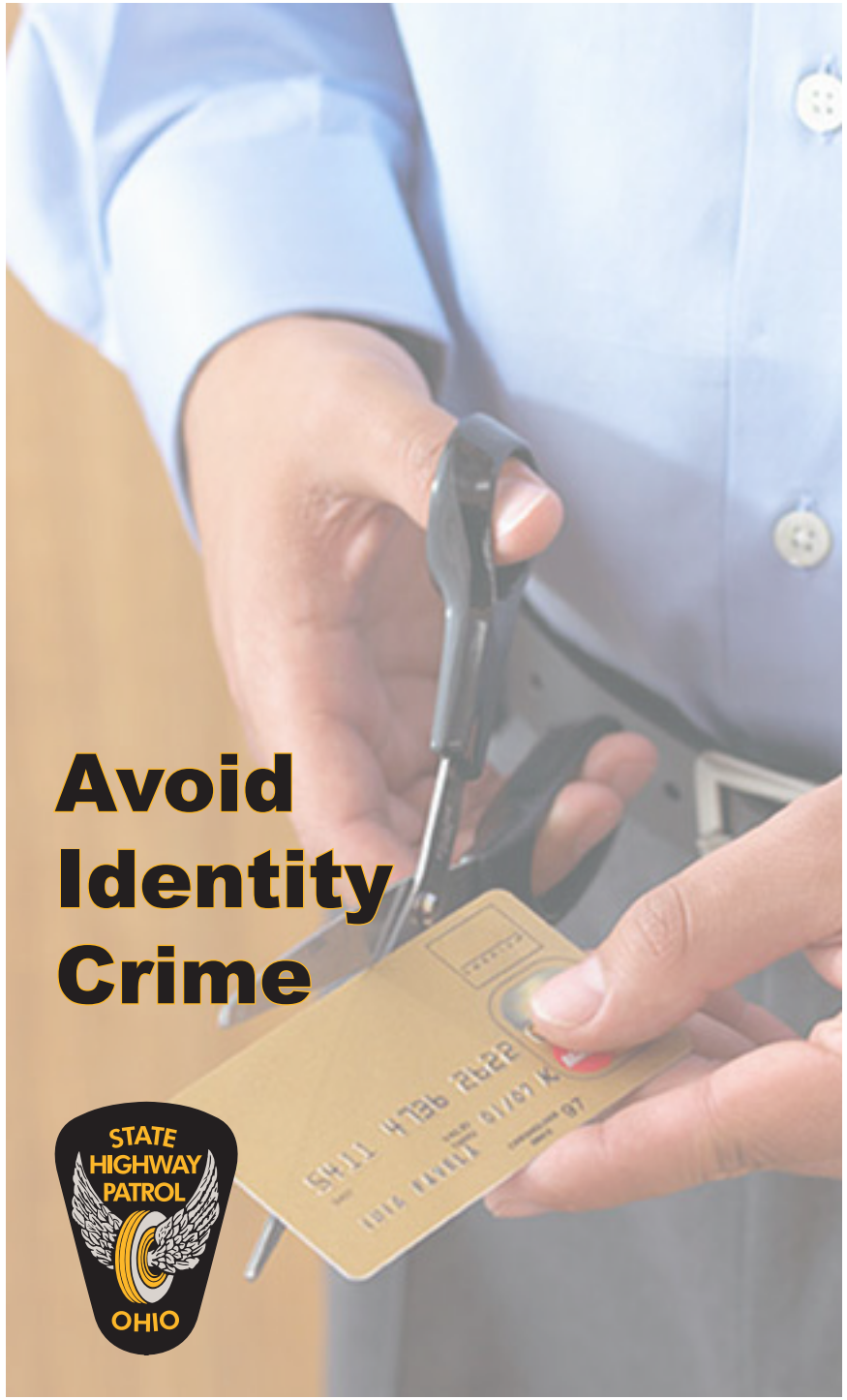
OHIO DEPARTMENT
OF PUBLIC SAFETY
SAFETY · SERVICE · PROTECTION

WWW.PUBLICSAFETY.OHIO.GOV

OHP 0523 5/16



Avoid Identity Crime

STATE HIGHWAY PATROL
OHIO

Social Media

Refrain from posting personal details on social media and restrict who can view your accounts. Do not “friend” people you don’t know. Abstain from using your social media accounts to sign into cell phone application and other websites.

Websites of Interest

Additional information and help may be obtained through:

1. U.S. Dept. of Justice - www.justice.gov
2. FBI - www.fbi.gov
3. U.S. Postal Service - www.usps.com
4. Federal Trade Commission - www.ftc.gov
5. Ohio Attorney General - www.ohioattorneygeneral.gov
6. Ohio State Highway Patrol - www.statepatrol.ohio.gov

Preface

Included in the mission of the Ohio State Highway Patrol is the commitment to investigate criminal activities involving State of Ohio interests. In that capacity, troopers and multi-agency task forces work together to detect and apprehend persons involved in **identity fraud** through the utilization of **state driver licenses and identification cards.** Armed with knowledge, you can help prevent identity fraud and recover more effectively if you become a victim of this pervasive crime.

Steps to avoid becoming

A Victim of an Identity Crime

Identity theft occurs when someone obtains important personal information, such as your Social Security number or banking or credit card account numbers, to commit fraud or theft. The goal of this brochure is to help you avoid becoming a victim of "identity theft."

Many identity crimes are either undetected or go unreported. Identity thieves are information seekers who don't need to steal your wallet. The Ohio State Highway Patrol has developed this brochure to offer steps you can take to reduce your risk of disclosing important personal information and of becoming a victim of identity theft.

Your personal identifying information can be accessed in a variety of ways. An impostor can use this information to open fraudulent credit card accounts, secure deposits on cars and housing, obtain employment opportunities, create insurance benefits, and rob retirement earnings. This form of financial sabotage can devastate your credit and require endless hours of telephone and written communication to resolve. In the meantime, you may experience difficulty writing checks, obtaining loans, renting apartments, and even getting hired. While following these precautionary steps is not a guarantee, it will reduce your chances of becoming an identity theft victim.

Reduce Access to Personal Identifying Information

To minimize the amount of information a thief can steal, do not routinely carry extra credit cards or your Social Security card, birth certificate, or passport in your wallet or purse.

To reduce the amount of personal information that is "out there," consider the following:

- Remove your name from the marketing lists of the three credit reporting bureaus: CSC Credit Services (Equifax Regional Office), Experian (formerly TRW), and Trans Union. This will limit the number of pre-approved offers of credit you receive in the mail. When in transit or tossed into the garbage, such solicitations are a potential target of identity thieves who use them to order credit cards in your name.
- Order your credit report once a year from each of the three credit bureaus. Check for inaccuracies or 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.

same with other sensitive information like credit card receipts, banking statements, phone bills, and so on. Home shredders can be purchased in most office supply stores.

Demand that your financial institution adequately safeguard your personal identifying information. Discourage your bank from using the last four digits of the Social Security number as your assigned personal identification number (PIN). Request that your bank remove account numbers from ATM receipts (many have already done so). Inquire whether they shred all paper records before discarding them. 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.

When you fill out credit or loan applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores have been known to be careless with customer applications or an employee at the business with "insider access" may retrieve your personal information to sell or use fraudulently. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by credit card if you think the business does not use adequate safeguards.

Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including your account number, telephone number, and driver license number. Never permit your credit card number to be written onto your checks.

When in public, be aware of your surroundings. Thieves commonly use a distraction in cramped public places, such as elevators, escalators and revolving doors to "bump and lift" your money, identification, and credit cards. Be especially cautious with bags and purses that can be easy targets for a thief to "grab and run."

Magazines, credit card companies, clubs and organizations, charities, manufacturers, and retailers make lists of subscribers, customers, members, and donors available to other businesses for a fee. Your information is reproduced and sold in countless ways. Exercise caution when making personal identifying information available (e.g., utilizing the Internet, sending a mail-in rebate/survey/warranty card, entering a drawing or sweepstakes, donating money, and even subscribing to magazine services).

If you have further questions or concerns, or if you would like additional information, please contact us at (614) 752-0234.

notice will explain whether disclosure of such information is required or requested, the use that will be made of the information, and what will happen if you refuse to provide all or any part of the information. You may wish to utilize an "assigned" driver license number rather than your Social Security number whenever possible. Assigned numbers are only available to holders of a non-commercial driver license.

Do not print your Social Security number on your checks. Don't let merchants hand-write your Social Security number on your checks because of the risk of fraud. Currently, there is no law against a merchant requiring you to divulge your Social Security number before accepting a check, so you may need to be assertive. Offering your assigned driver license number is usually an adequate substitute.

Order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) from the Social Security Administration every three years to check for inaccuracies or fraud. To request a PEBES application call or write:

Social Security Administration
Office of the Inspector General
550 Main St.
Cincinnati, OH 45202
Phone: 513-684-6496

Social Security Administration
Office of the Inspector General
1240 E. 9th St.
Cleveland, OH 44199
Phone: 216-522-7122

To download a PEBES application: www.ssa.gov

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 their billing systems 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 ("cramming"). Scrutinize your local, long distance, and cellular telephone bills each month for fraudulent or unauthorized charges. Be aware that some long distance telephone companies resort to deceptive tactics to switch your service without authorization ("slamming"). Contact your local telephone company to verify your long distance carrier and request a "freeze" on your account so it cannot be changed without your specific authorization.

Do not toss credit card convenience checks or pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. They can be used by "dumpster divers" to cash the checks or order credit cards in *your* name and mail them to *their* address. Do the

Credit Bureau	Report Fraud	Request Credit Report	Removal from Mailing Lists
CSC Credit Services (Equifax Regional Office) P.O. Box 740241 Atlanta, GA 30374-0241	888-525-6285 and write to: Fraud Victim Assistance Dept P.O. Box 740256 Atlanta, GA 30374	800-685-1111	800-567-8688 and write to: Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374
Experian (TRW) P.O. Box 9530 Allen, TX 75013	888-397-3742 and write to: National Consumer Assistance P.O. Box 9554 Allen, TX 75013	877 FACTACT	402-458-5247 and write to: Experian National Consumer Assistance Center 901 West Bond Street Lincoln, NE 68521
TransUnion P.O. Box 6790 Fullerton, CA 92634	800-680-7289 and write to: Fraud Victim Assistance Dept. P.O. Box 2000 Chester, PA 19016-2000	877-322-8228	888-567-8688 TransUnion LLC Name Removal Option P.O. Box 97328 Jackson, MS 39288-7328

- You may remove your name, home address, and home telephone number from many mailing and telephone lists through the Direct Marketing Association's Mail Preference Service and Telephone Preference Service. This service is available for individuals and "home" addresses only (not businesses). You will be removed from the Direct Marketing Association member lists for five years.

To remove your name and home address from national mailing lists, write:	To remove your name and phone number from national lists, write:
Direct Marketing Association Mail Preference Service P.O. Box 643 Carmel, NY 10512-0643	Direct Marketing Association Telephone Preference Service P.O. Box 1559 Carmel, NY 10512-1559

- Consider removing your name and address from telephone books, reverse directories, and city directories. By eliminating your name from these sources, you can reduce access to your personal information from places like the Internet (which mainly uses public information resources as a database), telemarketers, and identity thieves.

- Install a locked mailbox at your residence to reduce mail theft, or use a post office box.

- When you order new checks, consider removing "extra" information such as your Social Security number, driver license number, middle name, and telephone number. The less personal identifying information you make available, the more likely an identity thief will choose an easier target. Do not have new checks sent to your home mailbox. Pick them up at the bank instead.

- When you pay bills, do not leave the envelopes containing your checks at your home mailbox for the postal carrier to pick up. If stolen, your checks can be altered and then cashed. If stolen, credit card payments contain all the necessary information an identity thief needs. Never write your credit card account number or Social Security number on your checks when making a payment. Due to an increased risk of theft and vandalism, it is best to mail bills and other sensitive items at the post office, rather than from your residence or neighborhood drop boxes.

Credit Cards

Reduce the number of credit cards you use. Carry only one or two of them in your wallet. Cancel unused accounts. Even though you do not use them, these 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 your wallet or purse) so you can quickly contact your creditors if your cards become lost or stolen. Do the same with your bank accounts.

Never give out your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company **AND YOU INITIATED THE CALL**. Identity thieves have been known to call their victims with fake stories in order to obtain credit card information. ("Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your credit card number and expiration date to verify you as the lucky winner.")

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 their marketing and promotional lists that they sell or share with other companies. In addition, if any of your credit card issuers send random 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. Many times the consumer is unaware the checks were even issued. Your credit card billing statement should contain a different address for "correspondence" to the issuer. Do not send your requests to the same address where you send your credit card payments.

Watch the mail when you are expecting a new credit card that you have applied for, or a reissued credit card that has expired. Contact the issuer if the credit card does not arrive in a reasonable time.

One of the benefits for consumers using the Internet is the ability to electronically purchase products and services around the clock from the convenience of their home or office. One of the drawbacks is the potential for fraud and deception. Be very careful before you use a credit card on the Internet or provide personal information (such as your Social Security number or date of birth) on an electronic application.

Passwords and Personal Identification Numbers (PINs)

When creating passwords and PINs, do not use common words or numbers or anything else that could easily be discovered by thieves (e.g., the last four digits of your Social Security number, your birthdate, middle name, mother's maiden name, pet's name, address, consecutive numbers, etc.).

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 common passwords and PINs listed above.

Memorize all your passwords. Don't record them on anything in your wallet or purse.

Shield with your hand when using your PIN at a bank ATM or when making long distance phone calls with your phone card. "Shoulder surfers" may be spying nearby with binoculars or a video camera.

Social Security Numbers

Protect your Social Security number. It is the key to your banking and credit card accounts as well as insurance and health benefits, making it a prime target for identity thieves. Release it only when absolutely necessary or when required by law (e.g., tax forms, employment records, banking/stock/property transactions, driver/marriage/professional license applications, etc.).

When a government agency requests important personal information, including your Social Security number, a Privacy Act notice should accompany the request. (5 United States Code section 552a(e)(3)) This