Identity Theft
(An excerpt from the State of Ohio Passport Program)

Identity theft occurs when a criminal obtains and uses someone else's personal information such as credit card numbers, bank account numbers, insurance information and Social Security numbers to purchase goods or services fraudulently.

Identity theft is a crime at both the state and federal levels.

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 to check for inaccuracies of your account:
  - Trans Union [www.transunion.com](http://www.transunion.com) or at 800-916-8800.
  - Experian [www.experian.com](http://www.experian.com) or at 888-397-3742.
  - Equifax [www.equifax.com](http://www.equifax.com) or at 800-685-1111.
- Monitor your credit card statements regularly.
- Remove your name from the marketing lists of these credit-reporting agencies by calling the Credit Reporting Industry opt-out phone number at 888-567-8688.
- Remove your name from mailing lists by contacting the Direct Marketing Association at:
  Mail Preference Service
  Attention: Dept. 9301235
  Direct Marketing Association
  P.O. Box 6423
  Carmel, NY 10512
- Shred or destroy credit card statements, bills, insurance papers or bank statements before throwing them out.
- Carry only one or two credit cards in your wallet.
- When making credit card purchases, ask for the carbons if the retailer is not using carbonless forms.
- Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded in your credit report.
- Keep a list or photocopy of all your credit cards, so you can quickly contact your creditors in case your cards are lost or stolen. Do the same with bank accounts.
- Never toss ATM and credit card receipts in a public trash container.
- 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 or supply personal information online.
- Never give out personal or financial information over the phone.
- Thoroughly review all financial statements for any unusual activity. Immediately contact the company if an item looks suspicious.
- When creating passwords and PIN’s, do not use anything that could be discovered easily.
- Memorize all your passwords and PINs.
- Release your Social Security number only when absolutely necessary or required by law.
- Do not carry your Social Security card in your wallet.
- If you think an identity thief is using your Social Security number, call the Social Security Fraud Hotline at 800-269-0271.
- Be wary of anyone calling to “confirm” personal or financial information. Often, these are criminals trying to obtain those facts.