

Crime Prevention Tips:

We have identified several important points to keep you, your family and your home safe.

- Ensure your address is visible from every angle, to ensure a rapid response of emergency personnel. (reflective numbers are suggested)
- Secure your ladders and tools locked in the garage or storage shed.
- Conduct a home inventory of all personal belongings, recording the serial and model numbers. Keep this list in a fire-proof safe and a copy away from the home.
- Ensure that windows and doors are not blocked by large overgrown bushes or debris.
- All entry doors should have deadbolt locks to deter unauthorized access.
- Keep an extra set of keys with a neighbor or lock box rather than hiding a key outside the home.
- Secure sliding glass doors with wooden dowels, rods or pins to prevent the door from being lifted and opened.
- Install peepholes in all solid entry doors.
- Install motion sensor lighting around the house.
- Install a home alarm system
- When away contact the police department to have a vacation watch initiated.

Remember the four D's

DETECT

Identify any potential entry points that are obscured or easily forced open.

DELAY

The longer it takes to gain entry, the more likely the intruder will pass by.

DENY

Use proper locks and solid doors to prevent forced entry into the home.

DETER

Use lighting around the home, cut shrubs to allow easy view of windows and doors.

Identity Theft:

Identity theft is the stealing of another's personal information to engage in illegal activities. It is committed for many different reasons, such as financial fraud, to work illegally in this country or to commit crimes under another name. These are statistics from the Federal Trade Commission (FTC):

- Identity theft is considered the fastest-growing white-collar crime.
- Ten million individuals were victims of identity theft in 2002; that is 5 percent of the population in the United States.
- There are over 2000 victims per day that are estimated to lose between \$20,000 and \$30,000 per incident.
- In the next five years, it is estimated that one in four people will be a victim, or a relative of a victim of identity theft.
- Victims may spend an average of 175 to 200 hours repairing the damage of an identity theft incident.
- It can take 12 to 14 months before a victim becomes aware their identity has been stolen.

Being an identity theft victim can lead to a variety of problems including:

- Being hassled by creditors demanding payments on balances they do not owe.
- Ending up with a ruined credit report.
- Being unable to secure a job, rent an apartment, buy a car or obtain student loans.
- Being arrested for crimes the student did not commit.

Information Used for Identity Theft

Identity thieves are looking for sensitive personal information about an individual. There are many pieces of information that could be used. Some of the most common are:

- **Social Security number (SSN)** — The Social Security number was created in 1935 to keep an accurate record of earnings and pay retirement benefits on those earnings.
- **Date of birth (DOB)** — Date of birth, in conjunction with other pieces of information, can be used in many ways to compromise a person's identity.

- **Current and previous addresses and phone numbers** — Both can be used by an identity thief to pretend they are that person or to obtain more information about the victim.
- **Current and previous employment information** — Both can be used to jeopardize the victim's identity.
- **Financial account information** — This includes checking and savings accounts, credit cards, debit cards, and financial planning information.
- **Mother's maiden name** — In many instances, the maiden name of the victim's mother may be used as the password for financial accounts and is easily available through public record information.

Ways Information Can Be Obtained

Identity thieves can obtain personal information in a variety of ways. A thief may dig through trash looking for personal information, found on bills, credit card receipts, deposit slips or other discarded materials. He or she is also interested in the victim's junk mail, such as pre-approved credit card offers and convenience checks from a bank. Thieves will steal mail from a victim's mailbox. Some complete a change-of-address form to fraudulently receive a victim's bills and bank statements. Con artists will scam information over the phone, through the mail and over the Internet. Stealing a wallet or purse can provide a wealth of information. Sometimes a thief will watch a victim while they complete a transaction and memorize PIN numbers and passwords. Information unwittingly supplied to a vanity publication, or for a newspaper or magazine article, can compromise a person's identity. An unscrupulous employee with access to personal information may use the information kept in business records. There is also a wide variety of information easily obtainable through public records and companies that sell data.

Once the thief has some initial information, he or she can find additional information needed to:

- Apply for a driver's license.
- Obtain a credit report and use open lines of credit, or open new credit and bank accounts.
- Obtain cash through financial accounts.
- Purchase a car or other expensive items.
- Take a vacation.
- Create counterfeit checks.
- Commit a crime under the stolen name.
- Sell the information to other thieves.

The list could go on and on.

Prevention Tips

The following are tips to help avoid falling victim to identity theft.

Reduce Access to Personal Data

- Don't carry unnecessary information in wallets or purses.
- Don't lend IDs or other forms of identification.
- Don't leave mail out for the mail carrier, and use a locked mailbox for incoming mail.
- Be aware of who is given personal information. When asked to give personal information to someone, ask why it is needed, how the information is going to be used, and if there is alternate information that could be provided instead. Information should not be given to anyone that the consumer does not know.
- Opt out of mail offers with the credit reporting agencies and the Direct Marketing Association. Information on this is in Attorney General Jim Petro's *Protect Yourself Against Identity Theft* brochure.

Protecting Credit Cards

- Don't carry more than one or two credit cards.
- Limit the number of cards used, and cancel unused ones in writing.
- Pass by tables offering freebies to sign up for a credit card — buy a T-shirt instead.
- Keep a list of credit cards with the account numbers, expiration dates, and phone numbers of the customer service departments in a secure place in case the cards are stolen. This information will help when canceling the cards.
- **Never give account information over the phone.**
- Don't throw away receipts in public places, and do not leave receipts lying around.

Keep Passwords and PIN Numbers Secure

- Don't use the last four digits of a SSN, DOB, middle name, pet's name or consecutive numbers, boyfriend or girlfriend's name, name spelled backwards, or anything else easy to guess as a password.
- Don't carry passwords or PIN numbers in a wallet or purse or leave them lying next to the computer.
- Add extra protection to accounts with an additional password.
- Shield transactions when entering passwords and PIN numbers.

Protecting Social Security Numbers

- Do not give SSNs out to businesses just because they ask for it. There is no law against asking for a SSN and businesses may have a policy to require it for a transaction. However, ask why it is needed, what it will be used for, and if there is alternate information that could use instead. If the answer doesn't make sense, don't do business with the company.
- Request a randomly generated number for student ID numbers.
- Place a piece of removable, non-transparent tape over the SSN on identification cards. Keep these cards secure, and if they are lost or stolen, report it immediately.
- Do not carry SSNs in a wallet or purse unless absolutely necessary. Keep it in a secure place.

Some Additional Means of Protection Against Identity Theft

- Review all billing and account statements promptly.
- Reconcile financial accounts in a timely manner.
- Don't throw away sensitive material; destroy it. Shred all personal information.
- Beware of sending personal information over the Internet.
- Don't leave sensitive material in vehicles.
- Regularly review credit reports for suspicious activity.

What to Do if you are Victimized

The following information may be valuable if a student or student's family member falls victim to identity theft.

- File a police report. Keep a log of all conversations including the date and name of the person spoken with. Follow-up the conversation in writing and send certified mail with return receipt requested. File a complaint with the Federal Trade Commission at (877) FTC HELP (382-4357) or www.ftc.gov.
- Victims of identity theft can protect their credit report by contacting the fraud department of one of the major credit reporting agencies, and adding a victim statement informing the agency that their account was used fraudulently and they should be contacted to verify all new accounts. By sending notice to one of the major credit reporting agencies the victim will automatically be notifying the other two. Also, they will post a security alert on the credit file within 24 hours and electronically notify the other two. A fraud alert will be displayed by each credit reporting agency to all lenders or users. They will opt the victim out of pre-approved offers for two years and mail the victim a copy of his or her credit file. They will also work with the victim to verify the information and delete any fraudulent data. Credit reporting agencies are companies that collect and sell

information about the creditworthiness of individuals. The three major credit reporting agencies are Equifax, Experian, and TransUnion.

- A credit reporting agency collects information that it considers relevant to a person's credit habits and history. They use this information to assign a credit score, which indicates how creditworthy a person is. A person's "creditworthiness" is the degree to which a lender considers a person to be financially reliable enough to be given credit or lent money, and whether the lender considers them capable of repaying a loan. The most common measures used by lenders to determine an individual's creditworthiness are employment status, the sufficiency of current income to repay the loan, and credit history obtained from a credit reporting agency.

The toll-free telephone numbers for the Credit Reporting Agencies are:

Experian — (888) EXPERIAN [(888) 397-3742]

Equifax — (800) 525-6285

TransUnion — (800) 680-7289

For questions regarding identity theft, or for assistance with companies claiming money is owed to them that is not, contact Attorney General Jim Petro's Consumer Protection Section at:

Toll-Free: (800) 282-0515 toll-free

Locally: (614) 466-4986

TTY: (614) 995-7147 or (888) 567-6881

30 E. Broad St., 14th Fl.

Columbus, OH 43215-3400

www.ag.state.oh.us