**Identity Theft**

Every person who willfully obtains personal identifying information, e.g., name, address, date of birth, Social Security Number (SSN), mother’s maiden name, and uses that information for any unlawful purpose is guilty of a criminal offense. Identity theft is the fastest growing crime in the United States. Every year about 15 million people become victims. Everyone is vulnerable. Skilled identity thieves use a variety of methods to steal your personal information. These include the following:

* Dumpster diving. They rummage through trash looking for bills and other paper with your personal information on it.
* Skimming. They steal credit/debit card numbers with a special storage device when processing your card.
* Phishing and Whaling. See preceding tips on preventing Internet fraud.
* Changing your address. They divert your billing statements to another location by completing a change-of-address form.
* Stealing. They steal wallets, purses, mail (credit card statements, pre-approved credit offers, new checks, tax information, etc.), employee personnel records, etc.

Some of the things you can do to minimize your risk of identity theft are listed below.

***Protecting personal information***

Give out credit card, bank account, or other personal information only when you have initiated the contact or know and trust the person you are dealing with.  Beware of e-mail or telephone promotions designed to obtain personal information.

* Put strong passwords on your credit card, bank, computer, and online accounts.  Avoid using easily remembered numbers or available information like mother’s maiden name, date of birth, phone number, or the last four digits of your SSN.  Passwords should be more than eight characters in length, and contain both capital letters and at least one numeric character.  Use of non-dictionary words is also recommended.
* Select password reset questions whose answers cannot be found online or from other research tools.  Don’t compromise a strong password with an easily answered reset question like: What is your mother’s maiden name?
* Use different passwords for banking, e-commerce, e-mail, and other accounts.
* Memorize your passwords.  Don’t carry them in your purse or wallet.
* Keep personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home.
* Make sure that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier’s disk.
* Protect you health insurance cards like you would your credit cards.  If asked for your policy numbers or any other personal information in a doctor’s office make sure no one else is near enough to hear or see them.  And protect your Medicare card number as you would your Social Security number.
* Shred or tear up any documents with personal or financial information before throwing them in the trash.  Use a cross-cut shredder.
* U.S. Census workers will have an official U.S. Census Bureau badge with their name and an expiration date, and may have a Census Bureau bag. Ask to see the person’s identification and badge. Do not invite the person into your home. And do not give out any personal financial information. Any person asking for such information or asking for donations is not a U.S. Census worker. Nor is any person from another organization who says he or she is working for the Census Bureau. If you are unsure of the person’s identity you should call the Regional Census Center at **(800) 796-3748**.
* Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.

***Using credit cards***

* Cancel accounts you don’t use or need. Carry only the cards and identification you need when you go out.
* Never loan your card to anyone.
* Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
* Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won’t have access to the number.
* Notify your credit card companies and financial institutions in advance of any address or phone number changes.
* Bring home all credit card receipts and match them against your monthly statements. Look for charges you didn’t make. Dispose of them at home. Never toss your receipts in a public trash container.
* Call the credit card company or bank involved if a new credit card you applied for hasn’t arrived in a timely manner.
* Monitor the expiration dates of your credit cards and contact the card issuer if new cards are not received before your card expires.
* Report all lost or stolen credit cards immediately and request new cards.  In this case the federal Truth in Lending Act limits your liability to $50 of any charges made before you report your card lost or stolen.  Contact the issuer if replacement cards are not received in a reasonable time.
* Sign and activate new credit cards promptly on receipt. Or write “See ID” on the back of the card. Then a thief won’t have your signature.
* Never put your credit card number on a post card or on the outside of a mailing envelope.
* Make sure only the last four digits of your credit card number show up on your receipts.
* Cancel accounts you don’t use or need. Carry only the cards and identification you need when you go out.
* Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
* Ask your credit card company to stop sending blank checks. Call **(888) 567-8688**, the Consumer Credit Reporting Industry Opt-In and Opt-Out toll-free number, to stop pre-approved credit offers.

***Protecting your SSN***

* Examine your Social Security Personal Earnings and Benefits Estimate Statement for possible fraud. You will receive it about three months before your birthday each year.
* Provide your SSN only when it is required by a government agency, employer, or financial institution.  In a recent case a man received a call from a person who claimed to be a jury coordinator and said that a warrant has been issued for his arrest because he failed to report for jury duty.  When he protested that he never received a summons he was asked for his SSN and date of birth to verify the records.  Caught off guard he provided this information.  Instead he should have hung up realizing that court workers would never ask for a SSN or other personal information.
* In a variation of the above scam, the caller says that you’ve been selected for jury duty and asks you to verify your name and SSN. Remember, notification of jury duty is always done by mail.
* Never use your SSN for identification.  Don’t carry it or your Social Security card in your purse or wallet.
* Do not have your SSN or driver’s license number printed on your checks.  And never write your SSN on a check.

***Managing your accounts***

* Keep a record in a secure place of all your credit card, and bank and investment account and phone numbers for quick reference if identity theft occurs.
* Review your bank statements carefully. Match your checkbook entries against paid checks. Look for checks you didn’t write.
* Never leave transaction receipts at bank machines or counters, trashcans, gasoline pumps, etc.

***Carrying personal information in a purse or wallet***

* Carry only a driver’s license, cash, and one credit card. Don’t carry blank checks or a checkbook. Don’t carry anything with a PIN written on it.
* Keep a record of its contents. Photocopy both sides of your credit cards and driver’s license and keep them in a safe place at home.
* Don’t carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card is a safe place at home.
* If you carry a wallet in a purse, keep personal checks and credit cards in separate compartments and not in your wallet.
* Don’t carry personal information of your family members.
* Put a strong password on your Personal Data Assistant (PDA).
* Take the measures listed below for victims of identity theft if your wallet is lost or stolen. Don’t wait for someone to find and return it. These include filing a police report, reporting your credit and debit cards missing, closing checking accounts, having a fraud alert placed on your credit reports, notifying your medical insurance companies, reporting a missing driver’s license, etc.

***Using the mail***

* Deposit mail in boxes or slots inside a post office. Use an outside box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Also, do not leave mail for pickups from personal curbside boxes or cluster box units.
* Pick up your mail as soon as possible after it arrives in your personal curbside box or cluster box unit. If this is not possible, have a trusted friend or neighbor collect your mail, especially if you are expecting a check or credit card.
* Consider having new checks mailed to your bank for collection to avoid possible theft from your mailbox.
* Use a locked mailbox and make sure the lock works.
* Investigate immediately if bills do not arrive when expected, you receive unexpected credit cards or account statements, you are denied credit for no apparent reason, and you receive call or letters about purchases you did not make.
* Report the non-receipt of expected valuable mail by calling the sender and the Postal Inspection Service as soon as possible.

***Using an ATM***

* Use ATMs that are inside a store or a bank. If you use one that is outside it should be well-lighted and under video surveillance. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder’s financial information from an ATM transaction.
* Get off your cell phone and be alert when using an ATM.
* Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. If something doesn’t seem right, go to another machine.
* Look to see if there is anything in the slot where you insert your ATM card. Thieves place a small, hard-to-detect skimming device in the card slot to steal your PIN and other bank account information. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, contact the SDPD immediately. Don’t throw it away or keep it; that would make it look like you are running the scheme.
* Check for a false keypad that has been installed over the built-in one. False keypads stick out too far or look strange.
* Check the area around the machine for hidden cameras. To be safe shield your hand when entering your PIN so it can’t be seen by anyone near you or by a hidden camera.
* Memorize your PIN and keep it secret. Don’t write it down or keep it in your wallet or purse.
* Call the bank immediately if the ATM keeps your card.
* Monitor your bank statements and report any unauthorized activity immediately.

***Buying identity theft protection***

* You cannot buy absolute protection against identity theft. Beware of any such claims, especially regarding prevention of misuse of existing credit-card accounts, theft of medical records, and theft of personal information from employer’s personnel files.
* Before signing up for protection, be sure to understand what services are provided, what protections they afford, and how the personal information you provide is protected.
* Fraud alerts, which provide some protection against new-account fraud, do not provide absolute protection and only deal with about 17 percent of identity theft incidents according to a FTC survey released in 2007.

***Checking for possible identity theft***

* Obtain free copies of your credit reports from the three nationwide consumer reporting companies – Equifax, Experian, and TransUnion -- by visiting [**www.AnnualCreditReport.com**](http://www.annualcreditreport.com/) or calling **(877) 322-8228**.This is the ONLY source of free reports authorized under Federal law.  You can get one free report annually from each company.  Stagger your requests to obtain one every four months.  That way you can monitor your credit during the year.  Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit.  Contact the reporting company immediately if you see any inaccuracies. These companies may also try to sell you credit monitoring products or services for a fee.  Starting April 1, 2010 the FTC requires that any advertising for such products or services be delayed until after you get your free credit reports.
* Starting April 1, 2010 these websites will be required to print a disclosure that states the following at the top of each page that mentions free credit reports: “THIS NOTICE IS REQUIRED BY LAW. Read more at www.FTC.gov. You have the right to a free credit report from www.AnnualCreditReport.com or (877) 322-8228, the ONLY authorized source under federal law.” They will also have to include a clickable button to “Take me to the authorized source” and clickable links to www.AnnualCreditReport.com and www.FTC.gov.
* Place a security freeze on your credit reports.  This will protect you against fraud in new accounts by prohibiting the credit bureaus from releasing your credit reports to a potential creditor without your express permission.  Go to their websites for the procedures and fees for placing and lifting freezes. Their addresses are:[**www.equifax.com**](http://www.equifax.com/),[**www.experian.com**](http://www.experian.com/),and[**www.transunion.com**](http://www.transunion.com).
* Check your medical bills and health insurance statements to make sure the dates and types of services match your records. Read every letter you get from your insurer, including those that say “this is not a bill.” If you see a doctor’s name or date of service that isn’t familiar, call the doctor and your insurer.
* Once a year request a list of all benefits paid in your name by your health insurer. If the thief has changed your billing address you would not be receiving any bills or statements.

***Protecting your child’s identity***

* Provide your child’s SSN only when it is required by a government agency or financial institution. Never provide it for identification.
* Carry your child’s SSN or card in your purse or wallet only when you know you will need it.
* Teach your child never to give out personal information over the phone or on the Internet.
* Check to see if your child has a credit report. There should not be one unless someone has applied for credit using your child’s SSN. No minor should have a credit report.
* Watch your child’s mail for credit card applications, bills, or bank statements. They are signs that someone has started a credit history in your child’s name.
* Request that banks in which your child has an account remove his or her name from marketing lists.
* Report any suspected identity theft to the three nationwide consumer reporting companies and obtain copies of any credit reports in your child’s name and SSN. If your child does have a credit report ask to have all accounts, application inquiries, and collection notices removed immediately. Tell the credit issuer that the account is in the name of your minor child who by law isn’t permitted to enter into contracts.
* Take advantage of your rights under the federal Children’s Online Privacy Protection Act (COPPA). This law requires websites to get parental consent before collecting and sharing information from children under 13. COPPA covers sites designed for children under 13 and general audience sites that know certain users are under 13. It protects information that websites collect upfront and information that children give out or post later. It also requires these sites to post a privacy policy that provides details about the kind of information they will collect and what they might do with the information. You should: (1) know your rights, (2) be careful with your permission, (3) check out the sites your children visit, (4) review the sites’ privacy policies, (5) contact the site if you have any questions about its privacy policy, and report any site that breaks the rules to the FTC at [**www.ftc.gov/complaint**](http://www.ftc.gov/complaint).

***If you become or may become a victim of identity theft***

File a police report as soon as possible. Call GPD at (717)334-1168/1169. Then do the following:

* Set up a folder where you can keep a log of all your contacts and documents.
* Contact the Federal Trade Commission (FTC) to report the theft. Its Identity Theft Hotline is **(877) 438-4338**. Or visit its website at [**www.ftc.gov/idtheft**](http://www.ftc.gov/idtheft). The FTC is the federal clearinghouse of complaints of victims of identity theft. It helps victims by providing information to resolve financial and other problems that could result from identity theft. Its booklet entitled *Take Charge: Fighting Back Against Identity Theft* deals with bank accounts and fraudulent withdrawals, bankruptcy fraud, investment fraud, phone fraud, and other specific problems. It also describes the immediate steps victims should take and ways to minimize recurrences.
* Report the theft to the fraud units of Equifax at **(800) 525-6285**, Experian at **(888) 397-3742**, and TransUnion at **(800) 680-7289**. Ask to have a fraud alert placed on your credit reports. It will tell creditors to follow certain procedures before they open new accounts in your name or make changes to you existing accounts. In placing a fraud alert you will be entitled to free copies of your credit reports. Review them carefully. Look for inquiries from companies you haven’t contacted, accounts you didn’t open, and debts on your accounts that you can’t explain. Fraud alerts are good for 90 days and can be renewed. They are free.
* Alert your banks to close your accounts and open new accounts with new checks, ATM cards, PINs, and passwords. Also replace outstanding checks with new ones.
* Contact all your creditors by phone and in writing to inform them of the theft.
* Call the security or fraud departments of each company to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft.
* Contact the Social Security Administration’s Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at [**www.ssa.gov/oig**](http://www.ssa.gov/oig).
* Contact Pennsylvania DMV at: [**http://www.dmv.state.pa.us/identity\_theft/reporting\_fraud.shtml**](http://www.dmv.state.pa.us/identity_theft/reporting_fraud.shtml) for information on reporting an identity theft and other DMV frauds.
* Notify the U.S. Postal Inspector if your mail has been stolen or tampered with. Its number is **(626) 405-1200**.
* In the case of medical identity theft request a copy of your current medical files from each health care provider, and request that all false information be removed from your medical and insurance files.

Additional tips on avoiding and resolving identity theft problems are available on the Pennsylvania Attorney General’s Office website at: [**http://www.attorneygeneral.gov/**](http://www.attorneygeneral.gov/). Another useful website is that of the Identity Theft Resource Center (ITRC) at [**www.idtheftcenter.org**](http://www.idtheftcenter.org/). It contains information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft.  It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, a “Help, I’m a Victim of Identity Theft” button, and answers to frequently asked questions.  Its toll-free victim-assistance number is **(888) 400-5530**.

***If you are notified of a security breach involving personal information***

PA Senate Bill 712 establishes the "Breach of Personal Information Notification Act" and says a state agency, political subdivision, individual or business that operates in Pennsylvania and maintains, stores or manages personal consumer information on computer, must notify people if their security systems are breached.

Personal information under the bill includes an individual's first name, or initial, and last name; social security number; driver's license, or state-issued I.D., number; or a financial account number. Notification of the breach may be made in writing, by telephone, via email, or by a combination of email, posting on the entity's website, or notification to statewide media

Information on the Pennsylvania’s security breech law go to: [**http://www.attorneygeneral.gov**](http://www.attorneygeneral.gov)

For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse’s website at **www.privacyrights.org**.