What to do if you are a victim of Identity Theft

If you have been victimized by identity theft, you should take certain steps to protect yourself and minimize the consequences. Correcting the damage to your credit rating and good name may be a tedious and time consuming process.

If you are a resident of the Borough of Emmaus, you should file a report with the Emmaus Police Department. If you are not a resident of Emmaus, you should contact your local Police Department.

Step 1: Call all companies where you know fraud occurred:

Call and speak to someone in the fraud department. Explain that someone has stolen your identity and ask them to close or freeze the accounts. Change PINs, passwords, and logins and ask them to flag your accounts and contact you if there is any unusual activity.

You should create a file to store all of your paperwork in one location. You should create a log and document the dates, times, names and positions of everyone you talk to and everything you do during this process of correcting your name and credit history.

Step 2: Place a fraud alert by contacting one of the three credit reporting agencies and get your credit reports:

- www.Experian.com/fraud
  1(888)397-3742
- www.alerts.Equifax.com
  1(888)766-0008
- www.TransUnion.com/fraud
  1(800) 680-7289

Note: Only one of the three bureaus needs to be contacted as the bureaus notify each other, once a "Fraud Alert" is reported. After the "Fraud Alert" is placed on your credit, you will need to request a copy of your full credit report from each of three bureaus.

You can obtain a copy of your free credit reports from Equifax, Experian, and Transunion**:**

- www.annualcreditreport.com
  1(877)322-8228.

You should look over each credit report thoroughly, because each report may have slightly different information. Check all credit accounts and your previous addresses to make sure they are or were all yours.

Step 3: Report identity theft to the Federal Trade Commission (FTC):

- www.IdentityTheft.gov
  1(877)IDTHEFT

The Federal Trade Commission (FTC) is a law enforcement agency and based on the information that you provide to them, IdentityTheft.gov will create your Identity Theft Report and recovery plan.

You are not alone in this matter, and the Emmaus Police Department will assist you if you have any questions about the process described in this handout. Please call the number listed on the front of this pamphlet.

IDENTITY THEFT

A Pennsylvania Accredited Law Enforcement Agency

400 Jubilee Street
Emmaus, Pennsylvania 18049

Phone (610)967-3113
Fax (610)967-6288

www.borough.emmaus.pa.us

What is Identity Theft?

Identity theft is the unauthorized use of personal identifying information such as name, address, date of birth, and social security number. This information enables the identity thief to commit numerous forms of fraud, which include, but are not limited to opening new bank or credit accounts, purchasing homes and automobiles, applying for loans, social security benefits, tax fraud, renting apartments and establishing services with utility companies (cable TV, phone, electric etc.)

Who are the Victims of Identity Theft?

Identity fraud can claim many victims. Credit grantors, such as banks and retail merchants, are victims when they are not paid for the loans or goods sold. A person whose identity has been stolen is a victim, even if protected by insurance coverage or credit card reimbursement provisions. Although they may not have out-of-pocket losses, the Identity theft victim suffers from injuries to their reputations, and may have to go through lengthy and often agonizing processes to reestablish credit.

How Identity Theft May Occur?

People who commit identity theft do not fit a stereotype. The offender may or may not be known to the victim, and the method of operation varies. The following are only a few examples how criminals can obtain personal information:

DUMPSTER DIVING: Searching through trash for old mail, documents, or old personal computers and cell phones that have been thrown out where the data has not been wiped clean.

HACKING: Email or other online accounts to access your personal information, or hack into a company's database to access its records.

STEALING: Wallets, purses, mail, and records or data from their employers.

PHISHING: They pretend to be financial institutions, companies, or government agencies and send email or pop-up messages to get you to reveal personal information.

SCAMMING: They can pose as someone, and trick a company or person into releasing personal information by using phones, computers, the Internet or mail.

SKIMMING DEVICES: They steal credit / debit card numbers by using special devices when processing your card.

Preventing Identity Theft!

▪ Promptly remove mail from your mailbox and deposit outgoing mail at your local post office. Do not leave it in an unsecured location such as your home mailbox.

▪ Never give personal information over the phone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, unless YOU initiated the call. Protect this information and release only when absolutely necessary.

▪ Shred ALL discarded paperwork that contains personal identifying information, including pre-approved credit applications, utility bills, medical bills, and anything that contains even just your name and address.

▪ Stop pre-approved credit offers from being mailed to you, by calling all three credit bureaus and opting out of these programs. You should receive fewer pre-approved credit and loan applications.

▪ Do not respond to any emails where the sender is unknown to you. Many scams are initiated by sending an email that asks you to respond. When you respond, they may ask for your information, or can capture your personal information and passwords from your computer.

▪ Memorize your passwords, bank PIN's, and other numbers. Do not write them on cards or store them in your wallet or purse, or other areas where they may become accessible to others.

▪ Empty your wallet or purse and only carry the absolute minimum. Never carry your social security card with you unless you must do so for traveling. If you lose your purse or wallet, think how easy it would be for someone to assume your identity.

▪ Beware of mail, telephone, or computer scams that are disguised as promotions, instant prizes or computer repairs. These are used solely for obtaining personal information or money.

▪ Keep all computer software up to date, including but not limited to anti-malware software, and operating systems.

*****Be cautious and alert at all times. These are only some examples for preventing identity theft.**

Detecting Identity Theft!

Be alert to signs that require immediate attention:

▪Unauthorized charges or withdrawals.

▪Mail or bills that do not arrive as expected.

▪Merchants refuse your checks or you are denied credit for no apparent reason.

▪Receiving credit card or account statements that aren't yours.

▪Debt collectors call you about debts that aren't yours.

▪Unfamiliar accounts or charges on your credit report.

▪Medical providers bill you for services you didn't use.

▪Your health plan won't cover you because your medical records show you've reached your benefits limit.

▪A health plan won't cover you because your medical records show a condition you don't have.

▪The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.

▪You get notice that your information was compromised by a data breach at a company where you do business or have an account.

▪Monitor and inspect your credit report on a regular basis for unauthorized accounts and incorrect personal information. The law requires the credit reporting companies to provide you with a free copy of your credit report every 12 months if you ask for it.

*****Visit www.annualcreditreport.com or call 1(877)-322-8228 to request a copy of your report.**