TIPS TO SAFEGUARD YOUR INFORMATION

BetterWealth
enlightened discipline

Preventing Identity Theft

Anyone can become a victim of identity theft, whether young or old, so here are some guidelines that you can review to help reduce the likelihood of you becoming a victim. If you do become a victim, we have also provided advice on how you can go about reporting it.

1. If you use a debit or credit card, do not write the PIN on a piece of paper that you keep in your wallet or purse.
2. After making a payment, do not throw away your receipts, especially those that have your name on them and even parts of your debit or credit card number. If there are carbon copies, ask for those along with any receipts that may have incorrect charges on them. When you get your bank statements, compare your receipts to the purchases that you made to ensure that there are not any unauthorized transactions. It is also a good general rule to check your statements regularly to pick up on any suspicious transactions.
3. You can request that your credit be frozen in the event that fraudulent activity is detected. This will prevent any further release of your credit information to any business until the fraud has been investigated and clearance has been given. This means that if you try to buy something during the credit freeze, the company with whom you are doing business with will not be able to access your credit records until the issue has been sorted, meaning that they will not be able to do any business with you until then.
4. Do not throw expired credit cards, credit offers, bank account statements, and unwanted receipts into the garbage. Destroy them as best as possible, maybe even burn them, so that no one else can gain access to them. If you do not want to be so drastic, use a document shredder to shred sensitive documents and use a pair of scissors to cut up your debit and credit cards.
5. When withdrawing money at the ATM or making POS payments that require you to enter your PIN, shield the keypad with your free hand to prevent persons who may be looking over your shoulders from seeing your PIN.
6. If you are going to be away from home for an extended period of time, request that your mail delivery be placed on hold until you return home. Also check the post office to ensure that no one has tried to change your delivery address as ID thieves will attempt to route your mail to an unauthorized address.
7. Never carry your Social Security card in your purse or wallet. Do not write your Social Security number on checks either. Try to memorize it so that you do not have to write it down. When you must divulge it to anyone, make sure that it is an absolute necessity that the asker needs to know it.
8. If you receive unsolicited phone calls, mails, or online requests, do not provide any personal information to the requesting party.
9. If you are suspicious of someone having gained access to your personal information, check your credit report immediately. Keep on monitoring it regularly in the event that your suspicion lingers for a period of time.
10. Before using your computer to go online, install antivirus and firewall software. This will prevent people on the outside from accessing your computer remotely while protecting it from viruses that people may try to install on it when you access certain websites.

TIPS TO SAFEGUARD YOUR INFORMATION

11. Look out for phishing attacks. Phishing involves entering your personal information into forms or boxes that popup on your computer screen, these popups claiming to be from legitimate entities like banks and then your information is used for fraudulent purposes. Never enter your personal information into popups unless they are from websites that you trust and have dealt with in the past, like your financial institution's website. Also ensure that the website is a secure one that uses the HTTPS protocol which will ensure that any information you enter into the form will be encrypted as it travels over the Internet.
12. Know the cycles within which you receive your bills or financial statements. If any of them are suspiciously late, contact the senders immediately.
13. Do not leave your personal information lying around in the open. Store it in a safe place like a vault or safe.
14. Your passwords and other login information can be retrieved by ID thieves who may somehow get malware installed on your computer that captures those types of information. As such, it is important that you change them on a regular basis. To make it easier for you to remember to do that, you can, for example, set your computer to prompt you to change your password every month.
15. You can use the services of ID theft protection companies who would alert you of any suspicious activities on your account. Some of them will call you and ask if you are making a purchase at a specific business place. You can then confirm or deny that you are making the purchase. A classic case of a fraudulent purchase, for example, would be a wheelchair-bound 88 year-old man purchasing a motorcycle for himself. Though not totally foolproof, ID theft protection services add an extra layer of ID protection and the main players in the industry will pay you back any money you lose in the event that their service fails to prevent your ID from being stolen.

Guidelines for Senior Citizens

Unfortunately, quite a number of the persons who are affected by identity theft are senior citizens. If you are a senior citizen, or know any like your parents or grandparents, pay attention to these common ways in which their identities are usually stolen:

1. Many senior citizens are housed in long-term care facilities and nursing homes. Their personal information is on files that can be easily accessed by members of staff at those facilities. In addition, money, checkbooks, and bank statements that are kept in the senior citizen's rooms may be misused or stolen by dishonest staff members.
2. ID thieves, posing as telemarketers, make fraudulent calls to senior citizens offering medical services, senior citizen benefits, and other products. Senior citizens are normally asked to divulge personal information like their Medicare ID number, birth date, or Social Security number that the identity thieves use to profit for themselves.
3. Some medical service providers, with whom senior citizens have regular contact, can steal their personal insurance information to fraudulently bill senior citizens and health insurance companies. There are times too when the medical providers use the information to fraudulently obtain medical services in the names of senior citizens.

TIPS TO SAFEGUARD YOUR INFORMATION

4. There are false tax preparers who steal the Social Security numbers of senior citizens and sell them to scammers. Many of the scammers then use the SSN to gain information on senior citizens whom they later call telling them that that they have won monetary or other prizes, prizes they will only be able to collect after the senior citizens pay over some money to the scammers. Other ID thieves read the obituaries in order to file tax returns in the names of deceased individuals, a practice that later affects the spouses of the dead individuals who are unable to collect tax returns since the returns would have already been collected by the ID thieves.

Reporting Identity Theft

Most people walk around with a wallet or purse. It normally contains personally identifiable items that ID thieves would love to get their hands on. If you end up losing your wallet or purse, or think that you are a victim of identity theft, here are some things that you should consider immediately:

1. Make a report of the loss or your suspicions to the local police. When they issue you with a copy of the report, do not lose it. File the report safely so you can show it to retailers or creditors in the event you need evidence of the ID theft case. In this way, it will not go against your credit rating.
2. Contact your financial institution without delay. If you are unable to go in person to your local branch at that point, take a look on your financial account statement for their phone number and call them immediately. You may also check a phone directory for their number in the event that you are unable to access your account statement right now.
3. Implore the three credit bureaus to add a fraud alert to your account so that merchants will not approve new credit without your approval first. You can use an ID Theft Affidavit, a document that the credit bureaus and most major creditors have agreed to accept, to report the ID theft. This will help to protect your credit rating and good name.

By taking careful note of the information contained in this article, you will be able to prevent, or at least reduce, the possibility of becoming a victim of identity theft. In the event that you do become a victim, report the crime immediately to the appropriate authorities.

Reminders

We also ask that you notify us immediately if you change any of your contact information or suspect that your email account or financial account has been compromised. Please call (408) 659-2390 and we will assist you with this matter.