WAEPA® CHECKLIST

8 Ways to Prevent Identity Theft

Identity theft is a crime that impacts over 10 million adults in the U.S. every year. It can be as simple as someone opening an online account in your name, or as serious as applying for loans or credit cards using your information. They can steal your money, run up debt, destroy your credit rating, and even commit crimes using your identity. The reality is that we are all vulnerable to identity theft. To help you lower your risks and protect your financial security, we've put together a checklist on "8 Ways to Prevent Identity Theft."

1 Strengthen Passwords

Identity thieves seek password information to target your personal data. To improve your passwords, the key is to first get organized. How many different passwords do you currently use? Are they all different, or simply a variation of one another? You should use different passwords for every account and make them strong. Use a random mixture of numbers, letters, and symbols, and update them regularly. It might feel inconvenient, but the harder they are for you to remember, the harder they are for an identity thief to figure out.

2 Shred Everything

One of the most successful methods for identity theft is "dumpster diving." That's why you must shred everything that might be useful to them before you throw it away: credit card and bank statements, medical records, copies of tax returns, receipts, pre-approved credit card offers, and any junk mail with your name on it. File what you need for your records, and shred the rest.

CONTINUED >

WAEPA CHECKLIST

3 Don't Fall for Phishing

Identity thieves use "phishing" techniques to steal personal information directly from you. It can be as simple as someone calling you and pretending to be from your bank, credit card companies, stores you shop at, or even a government agency like the IRS. They do this phishing over the telephone, regular mail, and in emails. These are professional thieves and good at getting people to give them information. Don't fall for it. Never give them any personal information, such as account numbers or passwords. Legitimate businesses will never contact you directly to request this kind of information. Be mindful of official looking emails with links that tell you to "click here" for more details. Don't follow these links unless you are very confident that you are dealing with companies you know and trust. If you're not sure, go directly to the website of the company or group you normally deal with. Only then should you share your data.

4 Keep an Eye on Your Mail

Identity thieves love to steal your mail. It's one of the easiest ways for them to get personal information about you. A mailbox overflowing with mail can be an easy target. Make sure that you contact the post office and have them hold delivery of your mail when you're away, or ask a trusted neighbor to gather it for you. You might also think about getting a postal service approved "lockable" mailbox. If you don't receive mail you're expecting, contact the banks and credit card companies and tell them. And make sure that your mailing address is current with the all your financial institutions and the IRS.

5 Protect Your Social Security Number

Your social security number is the most important number you have – a gateway to all your personal information – and you must protect it accordingly. Never carry your Social Security card with you. Only carry it when you know you will actually need it. If a thief knows your name, address, and full Social Security number (sometimes even just the last four digits), they can easily assume your identity. Only give your number to companies or groups that you know and trust – and only when it is absolutely required. When you get your Social Security Personal Earnings and Benefit Estimate Statement, make sure that all the information is correct. If someone has stolen your identity, it may be apparent on your statement.

CONTINUED >

WAEPA CHECKLIST

6 Check Your Credit Reports

One of the easiest ways to protect yourself from identity thieves is to check your credit reports. By law, you may receive a free credit report each year from the three major credit bureaus (Experian, Equifax, and TransUnion). Review them thoroughly. Make sure that the information listed is directly related to you and your financial activities. Make sure that it's accurate and up-to-date. If you see something that you don't recognize, contact the credit bureau and ask for an explanation. This is your opportunity to dispute inaccurate information. You don't want to be denied credit because of fraudulent information or activity on your credit report.

7 Check Your Statements

When you get your credit card or bank statements, open them right away. Review, in detail, each statement and make sure that there aren't any unauthorized withdrawals or charges. Make sure that you recognize each and every withdrawal and charge. If you notice charges that don't look familiar or your balance seems off, this may be an indication that someone is using your credit card or bankcard without your approval. Contact your bank or credit card company immediately. Credit thieves will sometimes "test" your accounts to see if you are paying attention. They will start off by charging small amounts, then, when they are sure no one is watching their activities, they will move to big-ticket items. Stay vigilant.

8 Freeze Your Credit

This is very easy to do and can be a very effective way to reduce identity theft. Basically, you contact the three main credit bureaus Experian, Equifax, and TransUnion) and have them "freeze" your credit. This will restrict access to your credit records so new credit files cannot be opened. Once this is done, only you can unfreeze your credit. They will usually charge a small fee for this service. You can also "lock" your credit, which is a little easier, but it isn't as strong a protection as freezing. All three credit bureaus now allow you to lock or freeze your credit by using your smartphone. It's an added protection that you may find very useful when you think someone may be trying to steal your identity.