ALLONE HEALTH FAMILY OF EAPS

IDENTITY THEFT PROTECTION SERVICES

Here's what you need to know about Identity Theft Protection

If you're concerned about **data breaches** or **identity theft**, you may be considering signing up for identity theft protection services. Before you enroll, it's important to weigh the costs and benefits of various types of services. You also can compare them with free and low-cost services. The federal government's IdentityTheft.gov website provides free personal recovery plans and step-by-step guidance to help identity theft victims recover.

WHAT ARE IDENTITY THEFT PROTECTION SERVICES?

Many companies refer to their services as identity theft protection services . In fact, no service can protect you from having your personal information stolen. What these companies offer are monitoring and recovery services. Monitoring services watch for signs that an identity thief may be using your personal information. Recovery services help you deal with the effects of identity theft after it happens. Monitoring and recovery services are often sold together, and may include options like regular access to your **credit reports** or **credit scores.**

MONITORING SERVICES

There are two basic types of monitoring services — credit monitoring and identity monitoring.

Credit Monitoring tracks activity on your credit reports at one, two, or all three of the major credit bureaus — Equifax, Experian, and TransUnion. If you spot activity that might result from identity theft or a mistake, you can take steps to resolve the problem before it grows. Usually, credit monitoring will alert you when:

- ***a company checks your credit history***
- ***a new loan or credit card account is opened in your name***
- ***a creditor or debt collector says your payment is late***
- ***public records show that you've filed for bankruptcy***
- ***there is a legal judgment against you***
- ***your credit limits change***
- ***your personal information, like your name, address, or phone number, changes***

Credit monitoring only warns you about activity that shows up on your credit report. But many types of identity theft won't appear. For example, credit monitoring won't tell you if an identity thief withdraws money from your bank account, or uses your Social Security number to file a tax return and collect your refund.

Some services only monitor your credit report at one of the credit bureaus. So, for example, if your service only monitors TransUnion, you won't be alerted to items that appear on your Equifax or Experian reports. Prices for credit monitoring vary widely, so it pays to shop around.

Questions to ask credit monitoring service providers:

- ***Which credit bureaus do you monitor?***
- ***How often do you monitor reports? Some monitor daily; others are less frequent.***
- ***What access will I have to my credit reports? Can I see my reports at all three credit bureaus? Is there a limit to how often I can see my reports? Will I be charged a separate fee each time I view a report?***
- ***Are other services included, such as access to my credit score?***

Identity Monitoring alerts you when your personal information — like your bank account information or Social Security, driver's license, passport, or medical ID number — is being used in ways that generally don't show up on your credit report. For example, identity monitoring services may tell you when your information shows up in:

- ***change of address requests***
- ***court or arrest records***
- ***orders for new utility, cable, or wireless services***
- ***payday loan applications***
- ***check cashing requests***
- ***social media***
- ***websites that identity thieves use to trade stolen information***

To find out if your information is being misused, identity monitoring services must check databases that collect different types of information to see if they contain new or inaccurate information about you. For example, they might check the National Change of Address database to see if anyone is trying to redirect your mail. The effectiveness of the monitoring will depend on factors like the kinds of databases the service checks, how good the databases are at collecting information, and how often the service checks each database. There also may be information that a service cannot monitor. For example, most monitoring services can't alert you to tax or government benefits fraud, including Medicare, Medicaid, welfare, and Social Security frauds.

Questions to ask identity monitoring providers:

- ***What kinds of information do you check, and how often? For example, does the service check databases that show payday loan applications to see if someone is misusing my information to get a loan?***
- ***What personal information do you need from me and how will you use my information?***
- ***Are other services included with the identity monitoring service? Do they cost extra?***

IDENTITY RECOVERY SERVICES

Identity recovery services are designed to help you regain control of your good name and finances after identity theft occurs. Usually, trained counselors or case managers walk you through the process of addressing your identity theft problems. They may help you write letters to creditors and debt collectors, place a freeze on your credit report to prevent an identity thief from opening new accounts in your name, or guide you through documents you have to review. Some services will represent you in dealing with creditors or other institutions if you formally grant them authority to act on your behalf.

IDENTITY THEFT INSURANCE

Identity theft insurance is offered by most of the major identity theft protection services. The insurance generally covers only out-of-pocket expenses directly associated with reclaiming your identity. Typically, these expenses are limited to things like postage, copying, and notary costs. Less often, the expenses might include lost wages or legal fees. The insurance generally doesn't reimburse you for any stolen money or financial loss resulting from the theft.

As with any insurance policy, there may be a deductible, as well as limitations and exclusions. Also, most policies don't pay if your loss is otherwise covered by your homeowner's or renter's insurance. If you're interested in identity theft insurance, ask to see a copy of the company's terms and conditions.

ALTERNATIVES TO COMMERCIAL IDENTITY THEFT PROTECTION SERVICES

Here are some low-cost — or free — ways you can protect yourself against identity theft:

- **Monitor your credit reports for free**. Federal law requires each of the three major credit bureaus to give you a free credit report — at your request — each year. Visit AnnualCreditReport.com — the only authorized website for free credit reports. If you want to monitor your reports over time, you can spread out your requests, getting one free report every four months.

- **Review statements** for your credit card, bank, retirement, brokerage, and other accounts every month. Or log in and check them even more frequently. They can tip you to fraudulent charges on your accounts long before issues show up on your credit report.

- **Review the explanation of benefits (EOB) statements** you get from your health insurance providers. If you see treatments you never received, immediately tell your insurer and medical providers.

- **Consider placing a free credit freeze** — also known as a security freeze — on your credit files with the major credit bureaus. A credit freeze blocks anyone from accessing your credit reports without your permission. Because potential creditors can't check your reports, a credit freeze generally stops identity thieves from opening new accounts in your name.
  - To freeze your credit reports, you'll have to contact each of the credit bureaus separately. If you opt for a freeze, each time you need to allow a company to check your credit — for example, if you apply for a loan or an apartment — you'll have to lift the freeze.
  - If you request a freeze by phone or online, the credit bureau must place it within one business day and lift it within one hour. If you make the request by mail, the credit bureau must place or lift it no later than three business days after it receives the request.
  - If you want to both freeze your credit and get monitoring services, sign up for the monitoring service before placing the credit freeze. That way, the monitoring service can get access to your credit files. Otherwise, you may not be able to complete the service's account creation process. If you lift the freeze to give the service access, restore it as soon as possible.

- **Consider taking advantage of free identity theft protection services** that businesses and the government may offer you after a data breach. Check out any company online before enrolling. Some scammers send fake "free" offers to steal your personal information.

- If you believe you are at risk of becoming an identity theft victim — possibly because you received a data breach notice or your wallet was lost or stolen — you can **place a free, one-year fraud alert on your credit report.** The alert tells potential creditors and lenders to contact you directly and verify your identity before opening new accounts in your name. You can renew the fraud alert after one year, or remove it at any time.
  - To place a **fraud alert**, contact one of the three credit bureaus. The one you contact must tell the other two about your alert. You'll get a letter from each credit bureau confirming that it placed a fraud alert. The letter also will tell you that you are entitled to a free credit report — even if you already ordered your free annual credit report this year — and explain how to request the report. You will have to request a free report from each credit bureau.

- If you are already the victim of identity theft, you are entitled to an **extended fraud alert**, which lasts seven years. When you contact the credit bureaus to request an extended fraud alert , you'll need to include a copy of your Identity Theft Report, which you can get from IdentityTheft.gov.

IDENTITYTHEFT.GOV OFFERS FREE PERSONAL RECOVERY PLANS

Visit IdentityTheft.gov if you believe you have been the victim of identity theft, or if your personal information has been lost or exposed. IdentityTheft.gov is the federal government's free, one-stop resource for reporting and recovering from identity theft. The website, available in Spanish at RobodeIdentidad.gov , will provide you with a personal, interactive recovery plan tailored to your individual identity theft needs. It will:

- ***Walk you through each recovery step***
- ***Generate an Identity Theft Report and pre-filled letters and forms for you to send to credit bureaus, businesses, debt collectors, and the IRS***
- ***Adapt to your changing needs, provide you with follow-up reminders, and help you track your progress***
- ***Give advice about what to do if you're affected by specific data breaches***

IdentityTheft.gov has recovery plans for more than 30 types of identity theft, including tax-related identity theft and identity theft involving a child's information. Please check out this video to learn more about the website.

Contact the national credit bureaus to request fraud alerts, credit freezes (also known as security freezes), and opt outs from pre-screened credit offers.

EQUIFAX

Equifax.com/personal/credit-report-services
800-685-1111

EXPERIAN

Experian.com/help
888-EXPERIAN (888-397-3742)

TRANSUNION

TransUnion.com/credit-help
888-909-8872