Allstate IDENTITY PROTECTION

frequently asked questions

Want to know more about protection that keeps up with real life? We've got answers to many common questions here.

Don't see your question here?
Contact our support team at 800-789-2720 or visit myaip.com.

How do you protect my identity?

We know that tracking your own identity can be complicated and overwhelming, so we're here to take the burden off your shoulders so you can live your life.

We use our proprietary software to proactively monitor information you provide. Through Allstate Identity Protection, you will also have the power to create thresholds for your bank accounts, allowing you to receive alerts for suspicious financial transactions outside of your set limits. We monitor your credit reports and credit-related accounts to ensure no one is using your name fraudulently, and we monitor the dark web to check for compromised credentials and unauthorized account access. While we can't prevent fraud, we can and do alert you at its very first sign, then work to resolve the fraud and restore your identity.

How do you prevent my identity from being misused?

Our technology helps detect when an identity may be at an elevated risk for theft and allows us to help you take necessary precautions, including placing fraud alerts, credit freezes, and reviewing credit reports. We go beyond credit monitoring to search for suspicious activity, looking holistically at the financial accounts you use, the social media accounts you log into, and other data sources that could be compromised by others. This allows us to alert you of fraud at its earliest signs.

What type of safeguards are used to protect my personal information?

We know that protecting your information is of utmost importance. That's why we use security software to encrypt the information before and during its transmission through the internet. We only allow information to be submitted for transmission if your browser is compatible with our security software. If your browser is not compatible, you will receive a message indicating your transaction can be completed but at a lower level of security. No method of transmission over the internet — or method of electronic storage — is 100% secure, however. Therefore, we cannot guarantee its absolute security.

Allstate Identity Protection never sells your information to third parties.

AIP1070_OE2027_Subscriber FAQ_5.26.26

How do you compare with other services, like credit monitoring?

While our service includes credit monitoring, we know that credit is just one aspect of identity protection. We detect a more expansive range of digital threats beyond your credit accounts. Our identity monitoring looks for misuse not only of credit, but also of high-risk transactions (suspicious non-credit activity such as "payday" loans or forged signatures on documents) and compromised credentials on the dark web. This includes your financial and social media accounts.

Additionally, Allstate Identity Protection monitors the accounts you add, even from multiple financial institutions, in one place instead of relying on each bank's individual fraud monitoring system. You can even place thresholds for financial activity on all of your existing bank accounts, giving you greater insight into potentially fraudulent activity.

If you'd like more details on financial threshold monitoring, please contact our customer care team.

How do I know my identity is secure?

Every month, we'll email you updates with your Identity Health Status and any active alerts. You will also receive alerts when we detect an issue or suspicious activity. If that activity seems fraudulent or suspicious, please notify our customer care team by by calling our customer care team at 800-789-2720. In your member portal, you can also select 'Get support' on the alert you received or use the Identity Fraud Finder tool, located in the Identity Restoration section under the Guidance tile.

This is a new benefit offering from my employer. When does my coverage become effective?

If you receive Allstate Identity Protection as a voluntary benefit through your employer, your coverage will begin on your employer's effective date, which could be immediate.

While some features begin as soon as you enroll, for certain features to work, such as financial threshold monitoring, credit monitoring, and social media monitoring, you will need to enter your account or additional information for us to begin monitoring. When you log in, the corresponding tabs for each feature will be on the left side of your screen. Keep in mind, the more features you activate, the better we can help protect you. Please visit our Terms & Conditions for more information regarding product features.

How do I fully activate my features to make sure I'm totally protected?

Once your plan is effective, log in to your online account to activate all your features. Each additional feature has its own tab and will walk you through instructions to set it up. Setting up these additional features ensures that we can effectively monitor your identity for the first signs of fraud. The best part? Everything on your account is included in your plan, so there are no hidden charges or additional purchases.

To activate these features, visit **https://myaip.com/signin.** If you have trouble logging in, or have questions about these features, please contact our customer care team at 800-789-2720.

Does credit monitoring impact my credit score?

No, activating credit monitoring on your account is considered a soft inquiry, which does not impact your credit score, as it is informational only and not a credit application. This is different from a hard inquiry, which occurs when you apply for credit. A hard inquiry can impact your credit score.

What should I do if my identity is stolen or I am the victim of fraud?

If you're an Allstate Identity Protection member and suspect identity theft, there are several ways to get in touch with us:

- Call our customer care team at 855-821-2331.
- In your member portal, select "Get support" on the alert you received on your member portal.
- In your member portal, use our identity fraud finder tool located in the Identity Restoration section under the Guidance tile.

What if you can't reach me when you find out I've been the victim of fraud?

If your account features are fully up to date and enabled, you will receive an email and/or text message alert (according to your stated communication preferences) as soon as we detect fraudulent activity. You will also receive a monthly email showing your Identity Health status and any outstanding alerts that require your attention. You can also view any outstanding alerts directly in your account.

We strongly recommend you keep your account updated with your most recent contact information and preferred communication method, so that we can quickly alert you to any activity. If you have any trouble completing these tasks or have trouble receiving these communications, you can contact our customer care team here. If your account is not properly updated with your most recent contact information, you may not receive fraud alerts.

Do you provide a credit report?

Yes; we provide you with a monthly VantageScore 3.0 credit score, credit monitoring, and a free annual credit report; however, credit monitoring is only one component of our monitoring services. We believe that protecting your identity not only requires credit monitoring, but further actions like monitoring for compromised credentials, financial transactions, and dark web activity.

This is why Allstate Identity Protection is able to provide early alerts and comprehensive protection that other providers cannot.

Is the credit score you provide my FICO score?

The monthly credit score you see in your dashboard is not your FICO score. The score you see on your Credit Monitoring tab comes directly from TransUnion; our industry calls it your VantageScore 3.0 score, and it ranges from 300 to 850. Financial sectors commonly use your FICO score to determine credit worthiness.

FICO and VantageScore 3.0 scores both range from 350 to 850. While they both follow similar rules, a FICO score also accounts for your Equifax and Experian scores.

Should I place a fraud alert on my credit bureau files?

If you believe your identity has been compromised, or if your Identity Health status shows you are at high risk of identity theft, we recommend placing a fraud alert on your credit bureau files. A fraud alert is a notice that lets credit card companies and others who may extend you credit know that you may have experienced fraud, including identity theft, and that they should take extra steps to verify your identity before extending credit.

Keep in mind that even if you do place a fraud alert on your credit bureau files, additional fraud or identity theft could still occur. That's why we monitor from many different sources, to provide additional layers of security.

If you have Allstate Identity Protection and you're unsure as to whether to place a fraud alert, please contact our customer care team as soon as possible by calling 855-821-2331.

What is internet surveillance?

The underground internet, also called the *deep web* or *dark web,* is where cybercriminals store and sell Personal Identifiable Information (PII) illegally. Our dark web surveillance scans the dark web for your personal information, and scours an ever-evolving complex of more than 30,000 compromised machines, networks, and web services that Allstate Identity Protection and other leading cybersecurity firms identify. Our surveillance is specifically designed to identify personal information like a Social Security number, medical insurance card, or even an email address and alert you immediately if it's exposed.

What type of reimbursement is offered?

Your reimbursement benefits depend on your plan. Most plans include identity theft expense and stolen funds reimbursement, which may cover many fraud-related expenses due to identity theft, including stolen funds, lost wages, out-of-pocket expenses, and legal fees. In some cases, coverage may also extend to funds stolen from 401(k)s, HSAs, unemployment benefits, stimulus payments, and tax refunds. Before we reimburse stolen funds, we will first attempt to remediate the issue through our standard process.

Your plan may also include cyber coverage, which provides up to $50,000 in aggregate reimbursement for:

- Scams, digital crimes, and social engineering: Financial fraud losses resulting from a cybercrime event.
- Data recovery and system restoration: Expenses related to restoring systems and recovering data lost due to a hacking attack.
- Cryptocurrency crime: Loss of cryptocurrency in a hacking attack.
- Ransomware payments: Reimbursement for payments made to criminals during ransomware attacks.

What are each plan's reimbursement limits for identity theft expenses, 401(k) and HSA, and stolen funds?

For identity theft-related expenses, we will reimburse up to $1 million with Pro plan, $2 million with a Pro+ plan, and $5 million with a Pro+ Cyber plan.

For incidents of funds stolen from an investment account such as 401(k) or HSA, we will reimburse up to $50,000 with a Pro plan or up to $1 million with a Pro+ or Pro+ Cyber plan.

Before we reimburse stolen funds, we will first attempt to remediate the issue through our standard process. Exclusions include fraudulent withdrawals that happened prior to your Allstate Identity Protection coverage.

Will I still be covered if I leave my company?

If you leave your company and reside in the U.S., you can still keep your coverage. Simply contact a member of our customer care team and we'll walk you through the options. Keep in mind, pricing may vary.

Can I still enroll and receive protection if I currently reside in another country?

Our service is intended for use in the U.S. only. By using Allstate Identity Protection, you are confirming that you are in fact a U.S. resident. For more information, see our **Terms & Conditions.**

Do I have to activate all the features on my account?

No, but we highly recommend activating all of our features so we can better monitor your information. There are no additional costs in activating the features on your account.

What does scam and cyber coverage include, with a Pro+ Cyber plan?

For members with a Pro+ Cyber individual or family plan, we offer up to $50,000 for scams, digital crimes, and social engineering, cryptocurrency funds reimbursement, data recovery and system restoration coverage, and ransomware payment coverage.

Cyberbullying: We offer up to $100,000 for expenses related to removing harmful content, receiving psychological support, investigating the incident, making educational changes for children, and any lost income due to the incident.

Data recovery & system restoration: Reimburses expenses for recovering data and restoring systems that were lost due to a hacking attack.

Scam & social engineering: Reimburses for financial fraud loss that the insured sustains because of a cyber crime event. A cyber crime event includes wire transfer fraud, phishing attacks, or the theft of money or securities from a covered bank account resulting from a hacking attack.

Cryptocurrency: Reimburses for the loss of cryptocurrency that the insured sustains as a direct result of a hacking attack.

Ransom payment: Covers payments to criminals as a result of ransomware attacks.

Who is included in the family plan?

We offer a generous definition of family, which means there is no age limit or floor for enrolled relatives. Family members of any age can be added to your coverage, from toddlers and college-age children to older adults.

If you're enrolled in a family plan, you can add any family member who has a Social Security number and resides in the United States. This includes relatives aged 65 and older, even if they don't live with you or receive financial support from you.

Please note that adult family members, including spouses and dependents over age 18, must enroll in credit monitoring individually and complete identity verification. As the primary member, you can invite covered adult family members to create their own online accounts so they can access available tools and support directly.

What if a family member outside of my household wants to enroll?

Family coverage extends to your children, parents, in-laws, and grandparents (age 65+) regardless of where they live or whether they receive any financial support from our participants. Please call us at 800-789-2720 or contact your benefits department for more information.

Is there an age limit for children to enroll?

There is no age limit for children to enroll in Allstate Identity Protection, so everyone from infants to adult children you support are covered.

What should I do if I have questions after I enroll?

You can contact our customer care team with any questions you have **here**. Whether you need help logging in to your account, adding family members to your plan, or managing fraud, our team works in-house, and is available 24/7 to assist.

What internet browsers do you support?

We currently support the following internet browsers: The latest version of Chrome, Firefox, Safari, and Edge. An older version may not have security updates as the newest version. Also, our application may not be compatible with the older versions.

Do I need an email address to enroll? Or to manage my account?

Yes, an email address is required to enroll and manage your account.

Will I only receive an alert via email? Are text and phone an option?

You can choose to receive alerts via email, email and text, and text only. We do not currently provide alerts via phone call. To manage your contact preferences, log into your Allstate Identity Protection account, click your initials in the top-right corner and select Settings.

Do you have Spanish services?

Yes, we do. When you call in, please select the Spanish option to be routed to one of our Spanish-speaking specialists. Estamos felices de ayudar!