Allstate IDENTITY PROTECTION

frequently asked questions

We offer identity protection solutions for real life, which means we might already have an answer for any questions you might have.

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 predictive technology detects when an identity is at elevated risk for theft and allows us to help you take necessary precautions — including placing fraud alerts, credit freezes, and pulling credit reports. Our proprietary technology goes beyond credit monitoring, allowing us to catch fraud early, not after the damage has been done.

How do you compare to other identity protection or credit monitoring services?

While Allstate Identity Protection's service includes credit monitoring, monthly scores, and an annual credit report, we know that credit is just one aspect of identity protection. We detect a more expansive range of identity theft beyond the range of credit accounts. Allstate Identity Protection's identity monitoring looks for misuse not only of credit, but also of high-risk transactions (suspicious non-credit activity) and compromised credentials on the dark web.

Please note that unlike a bank, we do not monitor all transactions at every business, nor do we monitor for every possible transaction type. However, using Allstate Identity Protection's financial threshold monitoring will give you greater control over your existing bank accounts than your bank's fraud monitoring alone. We provide additional features like dark web monitoring for personal data and passwords, social media account takeover monitoring, child credit checks, and full-service restoration make Allstate identity restoration the logical choice for identity protection. If you'd like more details on financial threshold monitoring, please contact our Customer Care team.

Is it safe to give you personal information like my Social Security number?

Yes. We know that protecting your information is of the utmost importance, so all our employees, consultants, contractors, and vendors adhere to a comprehensive information security policy when interacting with Allstate Identity Protection and its information. Customer data is stored in a state-of-the-art data center (SSAE 18 SOC1 and SOC2 Type 2 accredited and with HIPAA-ready infrastructure). That data is only accessible via secure, encrypted connections.

Allstate Identity Protection never sells your information to third parties.

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 selecting "Not me" or calling 800-789-2720.

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

If you enroll directly on a site that we host, your coverage will begin on your employer's effective date, which could be immediately. If you receive Allstate Identity Protection as a voluntary benefit through your employer, please contact your benefits provider for your plan's effective date.

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.

When I activate credit monitoring, will it impact my credit score?

No, activating credit monitoring will not impact your credit score. Viewing your own report and activating monitoring on your Allstate Identity Protection portal is considered a *soft inquiry,* which does not impact your 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.

Once you activate credit monitoring, you will also be able to receive monthly credit scores and an annual credit report.

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

If you suspect you are a victim of fraud or identity theft, **contact our Customer Care team as soon as possible** — either by selecting "Not me" on the alert within your portal or calling 800-789-2720. We will ask you questions and research with you to determine if you have been affected.

Once you are in touch with us and have been confirmed as a possible victim, you will be assigned to a Restoration Specialist who will work on your behalf to manage your case and fully restore your identity. Our Restoration Specialists are not outsourced — they work in-house. Our Restoration Specialists are *FCRA (Fair Credit Reporting Act) & CIPA (Certified Identity Protection Advisor) certified.* They are experts in identity restoration and are committed to doing the legwork to restore your identity for you.

What if you cannot reach me when you find out I have been a fraud victim?

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

If your contact information was not included when you initially enrolled, you will receive a welcome letter in the mail with instructions for how to log in to your account, update your contact information, and fully enable all your features.

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, call us at 800-789-2720.

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?

We recommend placing a fraud alert if you believe your identity has been compromised or if your Identity Health Status shows your identity is at high risk of identity theft. Unlike our competitors, we monitor from many different sources instead of simply placing a fraud alert in the hope that it will prevent fraud.

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 is covered under your identity theft insurance policy?

Allstate Identity Protection's identity theft insurance policy covers the financial damages of identity theft, such as costs to file reports or place freezes, legal defense expenses, and lost wages incurred as a result of resolving the fraud. Please contact us for a full copy of the policy and stipulations.

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 $1 million.

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.

Who is included in the family plan?

The Allstate Identity Protection benefit is available to anyone with a valid Social Security number. Coverage can extend to you and all family "under roof or under wallet" as well as any family member 65 or older. You can even protect senior family members aged 65+ who don't live with you or who are not financially dependent up on you, like parents, in-laws and grandparents. Consult with our Customer Care team, or your benefits department for more details.

What if people outside of my household want to enroll?

For plan specifics and potential additional costs, please call us at 800-789-2720 or contact your benefits department for more information.

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

As long as you have a Social Security number, we can monitor your identity and alert you whether you're living abroad or domestically. However, at this time, we cannot monitor foreign bank accounts. We also cannot monitor non-U.S. addresses or addresses in U.S. territories like Guam and Puerto Rico. If you live abroad and have a registered U.S. address that matches the address the credit bureaus have on file, we may be able to monitor you, however any mismatch in personal identifiable information will render us unable to monitor you.

Will I still be covered if I no longer work at my company?

If you leave your company, you can keep your coverage. If you are leaving your company and would like to keep your coverage, please contact the Customer Care team. Pricing may vary.

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 is covered.

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

If you have any questions after you enroll, please contact our privacy experts, who are available at 800-789-2720 or clientservices@aip.com.

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 create my account and receive alerts?

Yes, an email address is mandatory to create your account, receive alerts, and manage your account. Your username for your account is your email address.

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. You can manage your contact preferences by clicking your name in the top right corner, selecting **Account Settings**, and setting your alert preferences.

Do you have Spanish services?

We have Spanish-speaking Customer Care team members and Restoration Specialists.

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 are the coverage limits for cyber insurance with a Pro+ Cyber plan? (Excludes Pro and Pro+ plans)

For members with a Pro+ Cyber individual or family plan, we will reimburse up to $100,000 for cyberbullying and 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: Covers 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.