PrivacyArmor by InfoArmor

Frequently Asked Questions

How do you monitor my identity?

We use our exclusive software to proactively monitor various sources for suspicious activity. With PrivacyArmor®:

- You will be able to set thresholds for your bank accounts, allowing you to receive alerts for suspicious transactions above your set limits.
- We will screen your credit reports and credit-related accounts to make sure no one is using your name fraudulently.
- We will monitor the dark web* to check for compromised credentials and unauthorized access.
- We will alert you at the very first sign of suspicious activity, then resolve the fraud and restore your identity.

We know that tracking your own identity can be time-consuming and worrisome, so we're here to take the burden off your shoulders.

*The dark web, also called the deep web or the underground internet, is where cybercriminals store and sell Personal Identifiable Information (PII) illegally.

How does InfoArmor prevent my identity from being misused?

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

InfoArmor

How does InfoArmor compare to other identity protection or credit monitoring services?

Credit is just one aspect of identity protection. We detect a more expansive range of identity theft beyond credit accounts. InfoArmor's identity monitoring looks for misuse of credit, high-risk transactions (suspicious non-credit activity), and compromised credentials on the dark web. We do not monitor all transactions at every business, nor do we monitor for every possible transaction type. However, using PrivacyArmor's financial threshold monitoring will give you greater control over your existing bank accounts than your bank's fraud monitoring alone. If you'd like more details on financial threshold monitoring, please contact the Privacy Advocate team at 800.789.2720.

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

Yes. We know that protecting your information is important, so all our employees, consultants, contractors, and vendors follow a comprehensive information security policy when interacting with InfoArmor and its information. Customer data is stored in a state-of-the-art data center (SSAE 16 SOC1 and SOC2 Type II accredited and with HIPAA-ready infrastructure). That data is only accessible via secure, encrypted connections.

InfoArmor 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 level* and any active alerts. You will also receive alerts at the time we detect an issue or suspicious activity. If that activity seems fraudulent or suspicious, please notify our Privacy Advocate team by selecting "Not me" or calling 800.789.2720.

*Your Identity Health level will confirm whether you are in good standing, or if you have alerts which need to be cleared from your account.

When does my InfoArmor coverage become effective?

Your InfoArmor benefit will become effective Janurary 1st when you elect coverage during Open Enrollment; or your date of hire or the first day of becoming benefits eligible if you elect as a new hire/newly eligible employee.

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

Once your coverage is in effect, log in to your online account at InfoArmor.com to activate all your features.
You will need your Member ID number, found in your welcome letter, to log in to the online portal. Each feature has its own tab and instructions for activating. In order to turn on some of the features, such as the credit monitoring portion of your coverage, you will need to provide your, and any covered family member's, social security number.
Everything listed on your account is included in your plan, so there are no hidden charges, or additional purchases required. If you have trouble logging in, or have questions about the features, please contact a Privacy Advocate at 1.800.789.2720.

Who is included in the family plan?

Those you financially support or who live under your roof are covered under the family plan.
The PrivacyArmor benefit is available to those that have a Social Security number. Consult with a Privacy Advocate or your benefits department to determine if your family members are eligible for coverage. There is no age limit or floor for enrolled family members, so from infants to adult children you support, your whole family is covered.

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

Activating credit monitoring *will not* impact your credit score. Viewing your own report and activating monitoring on your PrivacyArmor portal is considered a soft inquiry, which does not impact your score, as it is informational only and not a credit application. A hard inquiry, which occurs when you apply for credit 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 with no impact to your credit rating.

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, please contact our Privacy Advocate team as soon as possible, either by selecting "Not me" on the alert within your portal or calling 800.789.2720. Your Privacy Advocate will ask you questions and research with you to determine if you are a victim.

Once you are in touch with a Privacy Advocate and have been confirmed as a possible victim, you will be assigned to a Remediation Specialist who will work on your behalf to manage your case and fully restore your identity. Our team members are not outsourced — they work in-house. Our Remediation Specialists are Certified Identity Theft Risk Management Specialists (CITRMS®), who are experts in identity restoration and are committed to doing the legwork to restore your identity for you.

What if my Privacy Advocate cannot reach me when they find out I have been a fraud victim?

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 your account features are current and enabled, you will receive an email or text message alert (depending on 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; and you can also view any outstanding alerts in your online portal.

Do you provide a credit report?

We provide you with a monthly VantageScore 3.0 credit score, credit monitoring, and a free annual credit report.

How does the VantageScore 3.0 differ from my FICO score?

The VantageScore 3.0 you see on your Credit Monitoring tab comes directly from TransUnion 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 have range from 350 to 850, and while they both follow similar rules, a FICO score also accounts for your Equifax and Experian scores.

If you are building your credit, it is important to look at the same credit score type, as not all scores are measured the same. To get a better idea of where your credit score stands, we encourage you to review the monthly changes to the VantageScore 3.0 score we provide in your PrivacyArmor portal.

Before opening a line of credit or taking out a loan, it's always best to ask which credit score the financial institution will use to determine credit worthiness. Please note, VantageScore 3.0 replaced Vantage score which went up to 990.

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 score shows your identity is at high risk of identity theft. Your Privacy Advocate will walk you through the necessary steps to complete this. We monitor from many different sources instead of simply placing a fraud alert in the hope 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 InfoArmor and other leading cybersecurity firms identify. Our surveillance is specifically designed to find identifying personal information like a Social Security number, medical insurance card, or even an email address and alert you immediately.

What is a Digital Exposure Report?

Your Digital Exposure Report is a summary of what a real-time deep internet search finds about you. The report also shows how vulnerable your online presence could be and provides tips for you to better secure your information. Please note that the Digital Exposure Report is not a credit report, so you may see search results for people with a similar name to yours. The less information you see on your Digital Exposure Report that matches you, the better!

What is covered under your identity theft insurance policy?

InfoArmor's identity theft insurance policy, which is including with your coverage, 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 at 1.800.789.2720 for a full copy of the policy and stipulations.

How does your retirement account, HSA, and stolen funds reimbursement plan work?

Before we reimburse stolen funds, we will first attempt to remediate the issue through our standard process.

For incidents of funds stolen from an investment account such as 401(k), 403(b), or HSA, we will reimburse up to $50,000. For incidents of funds stolen from other sources, we will reimburse up to $50,000.

The max total that we will reimburse an individual in one year is $75,000. The max total that we will reimburse a family in one year is $150,000.

Reimbursement covers only the first fraudulent withdrawal, and to be eligible for reimbursements, you must have Financial Transaction Monitoring enabled on the affected account at the time of the fraudulent withdrawal. Exclusions include fraudulent withdrawals that happened prior to your PrivacyArmor coverage.

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 Privacy Advocate team. Pricing may vary.

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

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

Do you have Privacy Advocates who can assist in other languages?

We have Spanish-speaking Privacy Advocates and Remediation Specialists. Additionally, InfoArmor has a third-party language line for languages other than Spanish.

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

If you have any questions after you enroll, please contact our Privacy Advocates, who are available 24/7, at 1.800.789.2720 or clientservices@infoarmor.com.

What internet browsers do you support?

We currently support the following internet browsers: Firefox 17+, Chrome 25 +, Safari 5.1+, and Internet Explorer 11. We recommend you update your browser if it is older than those we support, as older versions may not have security features as the newest versions.

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

Yes, an email address is mandatory to receive alerts and manage your account.

How will I receive alerts?

You can choose to receive alerts via email, text, or email and text, and text only. You can manage your contact preferences by clicking your name in the top right corner of the portal, selecting Account settings, and setting your alert preferences.

What if I want to keep my account hidden from my family members, so they can't view my personal information, such as credit?

You will need to contact our Privacy Advocate team. They can create separate login information for you and your family members, allowing you to keep your personal information private.