PrivacyArmor

Protect today.
Thrive tomorrow.

Get complete identity protection with PrivacyArmor Plus® so you can focus on what matters most.

Your identity is made up of more than your Social Security number and your bank accounts. That's why PrivacyArmor Plus does more than monitor your credit reports and scores. We safeguard your personal information, the data you share, and the relationships you treasure.

And now PrivacyArmor Plus is better than ever. We've teamed up with Allstate to provide the next generation of protection. Our new proprietary tools stay one step ahead — allowing us to catch fraud as it happens. In the event of wrongdoing, you have a dedicated Privacy Advocate® available 24/7 to fully manage your recovery and restore your identity.

- ✓ **Identity monitoring and alerts**
- ✓ **Full-service remediation**
- ✓ **Identity theft reimbursement†**
- ✓ **iOS and Android app**

Due to spikes in COVID-related cybercrime, your employer is now offering complimentary identity protection through December 31, 2020 if enrolled during open enrollment in JUNE & JULY

For more information visit

www.BenefitsSelection.com/richland-county-school-district-one

Sign up by 7/31/20 to be eligible for free coverage.

PrivacyArmor Plus

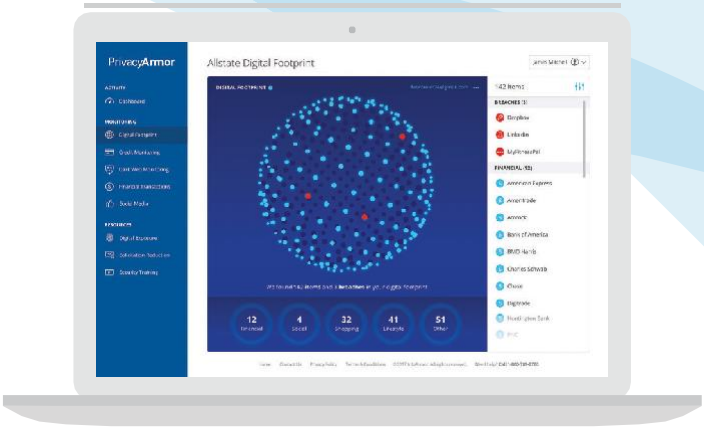
Plans and pricing starting 1/1/2021

$ 9.95 per person / month
$17.95 per family / month

InfoArmor
an Allstate company

The most comprehensive identity protection plan available

- Run your personalized Allstate Digital Footprint and see your digital exposure
- Check your identity health score
- View, manage, and clear alerts in real time
- Monitor your credit scores and reports for any changes or errors
- Receive alerts for cash withdrawals, balance transfers, and large purchases from any linked bank account
- Monitor linked social media accounts for questionable content and signs of account takeover
- Reduce solicitation attempts by opting out of credit **card offers, telemarketing calls, commercial mail and** email, and unrequested coupons
- Protect your account with biometric authentication security in iOS and Android
- Get reimbursed for stolen 401(k) & HSA funds; we'll also advance fraudulent tax returns †



NEW!
Allstate Digital Footprint™

All the incredible things you can do online require something from you — data. A "digital footprint" is a collection of all the data you've left behind that might **expose your identity. Our new tool offers a simple way** for you to see and secure your information, and help stop identity theft before it starts.

How it works

1 Enroll in PrivacyArmor Plus
You're protected from your effective date. Our auto-on credit monitoring alerts, and support require no additional setup.

2 Get to know us
Explore additional features in our easy-to-use portal. The more we monitor, the safer you can be.

3 We're on the job
Our human operatives see more — like when your personal information is sold on the dark web. If you've been compromised, we alert you.

4 We'll do the heavy lifting
In the event of identity theft or fraud, Privacy Advocates® are available 24/7. They won't stop until you're in the clear.

5 We've got your back
Our $1 million identity theft insurance policy covers out-of-pocket costs associated with identity restoration.†

InfoArmor
an Allstate company

PrivacyArmor Product features

Identity and credit monitoring

Proactive monitoring helps stop fraud at its earliest sign and enables quick restoration for minimal damage and stress.

- **Enhanced identity monitoring**
  Our proprietary monitoring platform detects high-risk activity to provide rapid alerts at the first sign of fraud.
- **Dark web monitoring**
  Our bots and human intelligence operatives scan closed hacker forums for compromised credentials.
- **High-risk transaction monitoring**
  We send alerts for non-credit-based transactions like student loan activity and medical billing.
- **Account activity**
  You are alerted when unusual activity on your personal banking accounts could be a sign of account takeover.
- **Financial activity monitoring**
  Alerts triggered from sources such as bank accounts, thresholds, credit and debit cards, 401(k)s, and other investment accounts help you take control of your finances.
- **Social media monitoring**
  We keep tabs on social accounts for everyone in the family, watching for vulgarity, threats, explicit content, violence, and cyberbullying. We monitor for account takeovers that could lead to costly reputation damage.
- **IP address monitoring**
  We scan for malicious use of your IP addresses. IP addresses may contribute to a profile of an individual, which — if compromised — can lead to identity theft.
- **Lost wallet protection**
  Easily store, access, and replace wallet contents. Our secure vault conveniently holds important information from credit cards, credentials, and documents.
- **Solicitation reduction**
  We aid you in opting in or out of the National Do Not Call Registry, credit offers, and junk mail.
- **Digital exposure reports**
  You can see and identify where your personal information is publicly available on the internet.
- **Credit monitoring and alerts**
  We alert for transactions like new inquiries, accounts in collections, new accounts, and bankruptcy filings. PrivacyArmor Plus also provides credit monitoring from all three bureaus, which may make spotting and resolving fraud faster and easier.
- **Data breach notifications**
  We send alerts every time there's a data breach affecting you directly so you can take action immediately.
- **Credit assistance**
  Our Privacy Advocates will help you freeze your credit files with the major credit bureaus. You can even dispute credit report items from your portal.
- **Sex offender registry**
  Our monitoring system shows if a sex offender is registered in a nearby area.
- **Mobile app**
  Access the entire PrivacyArmor portal on the go! Available for iOS and Android.

Product features

(continued)

Best-in-class customer care

Should fraud or identity theft occur, in-house Privacy Advocates are available 24/7 to fully restore compromised identities, even if the fraud or identity theft occurred prior to enrollment. And with a $1 million identity theft insurance policy — including reimbursement for HSA and 401(k) accounts† — you can rest assured that your identity is fully protected.

Full-service case management and resolution

We fully manage your restoration case, helping you save time, money, and stress.

Highly trained and certified Privacy Advocates

Our Privacy Advocates are trained and certified to handle and remediate every type of identity fraud case. When resolving complex cases of identity theft, our satisfaction score is an industry-leading 100%.

24/7 U.S.-based customer care center

We believe customer care is an essential part of our team. Our support center is located directly in our corporate headquarters, and our Privacy Advocates are available 24/7.

$1 million identity theft insurance

If your fall victim to fraud, we will reimburse your out-of-pocket costs.†

Stolen funds reimbursement

We'll reimburse you for stolen funds up to $1 million, including stolen 401(k) and HSA funds. We'll even advance tax refunds.†

Our proprietary technology solutions

We're reinventing protection by helping you see who has your data and prevent identity theft before it starts.

Allstate Digital Footprint

A digital footprint is a collection of all the accounts a person has opened, and information they've left behind that might expose them to risk. The Allstate Digital Footprint offers a simple way for you to see and secure your information, and is our next step in reinventing digital and identity protection.

Operative-sourced intelligence

We go beyond artificial intelligence and dark web "scans." Unlike other identity protection services, we harness a network of experienced human operatives to find what others can't. This exclusive combination is unique to InfoArmor and provides insight not only into the dark web but also invitation-only hacker forums. This helps us stay a step ahead of hackers and stop identity theft before it starts.

†Identity theft insurance underwritten by insurance company subsidiaries or affiliates of Assurant. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policy described. Please refer to the actual policy for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

PrivacyArmor is offered and serviced by InfoArmor, Inc., a subsidiary of The Allstate Corporation.

InfoArmor
an Allstate company

PrivacyArmor by InfoArmor

Frequently Asked Questions

How do you protect my identity?

We use our proprietary software to proactively monitor various sources. Through PrivacyArmor®, 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 resolve the fraud and restore your identity.

We know that tracking your own identity is cumbersome and fraught with unknowns, so we're here to take the burden off your shoulders so you can live your life.

How does InfoArmor 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 as it happens — not after the damage has been done.

InfoArmor

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

While InfoArmor'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. InfoArmor'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 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.

Is it safe to give InfoArmor 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 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 when 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.

When does my InfoArmor coverage become effective?

If you enroll directly on an InfoArmor-hosted site, your coverage will begin on your employer's effective date, which could be immediately. If you receive InfoArmor 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 signin.infoarmor.com. If you have trouble logging in, or have questions about these features, please contact a Privacy Advocate at 1.800.789.2720.

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 PrivacyArmor 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, 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 Privacy Advocates are not outsourced — they work in-house. Our Remediation Specialists are Certified Identity Theft Risk Management Specialists (CITRMS®). They 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?

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.

(continued on next page)

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 through the postal 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 InfoArmor 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 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. Comparing a FICO score to a VantageScore 3.0 is like comparing rice to pasta; 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 what credit score the financial institution will use to determine credit worthiness. Your bank may be pulling a different type of score (one that has a different low and high) than the one

(continued on next page)

PrivacyArmor provides. For example, your bank may have pulled a VANTAGE score if it was assessing your eligibility for a financial product or loan. A VANTAGE score goes up to 990, while the VantageScore 3.0 score PrivacyArmor provides tops out at 850. This is why your credit score may differ from other sources.

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. Unlike our competitors, 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 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.

How does your 401(k), 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) 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.

Who is included in 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.

What if people outside of my household want to enroll?

For plan specifics and potential additional costs, please call our Privacy Advocates at 1.800.789.2720 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 Privacy Advocate team. Pricing may vary.

Is there an age limit for children to enroll?

There is no age limit for children to enroll in PrivacyArmor. There is no age limit or floor, so from infants to adult children you support, your whole family is covered. However, Credit Monitoring is currently not available for children under 18 years old.

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.

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.

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

Please contact our Privacy Advocate team. They will be able to create separate login information for you and your family members so you can keep your personal information private.

Do you have Spanish services?

We have Spanish-speaking Privacy Advocates and Remediation Specialists.

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

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

The risk and impact of rising unemployment fraud

Pandemic-related unemployment fraud is rapidly increasing, as jobless numbers climb and more people file for unemployment benefits. Scammers take advantage of stolen personally identifiable information (PII), such as Social Security numbers or home addresses, to create convincing false unemployment claims. Due to years of pre-pandemic data breaches, these key data points are often readily available to criminals on the dark web.

The risk is widespread and increasing:

40M unemployment claims were filed over ten weeks[1]

$1.6M in phony claims were found in the state of Washington, halting unemployment payments for two days[2]

$13.4M in coronavirus-related fraud has hit Americans in 2020, according to the FTC[3]

Take a closer look at the ongoing impact:

Top 3

Unemployment fraud recently escalated to one of the top three most reported types of fraud at InfoArmor

3

new unemployment fraud cases discovered daily, on average, over the past 72 days

166%

increase in tax fraud cases

InfoArmor
an Allstate company

It's more critical than ever to get protection from the lasting effects of unemployment fraud.

How unemployment fraud can impact employees:

- Discovering identity theft makes 85% of victims feel worried, angry and frustrated[4]
- Exposed PII increases potential for additional fraud — 21% of fraud victims have been targeted multiple times[5]
- Increased potential for problems with the IRS, due to suspected under-reporting of income

How unemployment fraud can also impact employers:

- Distraction and stress increases the potential for absenteeism, threatening overall productivity
- Stolen employee PII could also be used to access an employer's sensitive client or customer information
- Increased Human Resources administrative burden

How can InfoArmor help?

24/7 access to expert full service remediation and restoration in the event of fraud

We work directly with the victim when remedying identity theft claims, so there's no input needed from HR staff

Our unique tools, comprehensive monitoring, and alerts encourage and empower employees to proactively monitor their PII and lessen the occurrence and impact of fraud

Coverage comes with critical alerts for financial transactions, new account openings, credit inquiries, address changes, and more

We provide identity theft insurance to cover a member's lost wages, legal fees, medical records request fees, CPA fees, child care fees, and more†

1: CNBC, "Jobs data shows millions went back to work but unemployment rate for May is still expected at 20%," May 2020
2: Krebs on Security, "U.S. Secret Service: 'Massive Fraud' Against State Unemployment Insurance Programs," May 2020
3: FTC, "COVID-19 scam reports, by the numbers," April 2020
4: Identity Theft Resource Center, "The Aftermath: The Non-economic Impacts of Identity Theft," 2018
5: CNBC, "The latest ways identity thieves are targeting you — and what to do if you are a victim," February 2020

†Identity theft insurance underwritten by insurance company subsidiaries or affiliates of Assurant. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

InfoArmor®
an Allstate® company

Current Statistics

$13.4M
Lost by Americans to coronavirus-related fraud since January[1]

18M
COVID-19 emails intercepted by Google last week[3]

30,000%
Increase in phishing and malware targeting remote users[2]

70,000
Suspicious newly registered domains related to COVID-19[4]

Source:
1 Federal Trade Commission
2 https://www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks
3 http://digitaledition.chicagotribune.com/infinity/article_share.aspx?guid=e7d5f241-9fd4-468a-ac60-f4269a7c2f3a
4 https://www.cnbc.com/2020/04/15/coronavirus-cybercriminals-are-targeting-people-through-phishing-scams.html