Northwestern University Identity Protection Coverage

1. How did Northwestern select InfoArmor?
   Earlier in the year, we began a search for a more comprehensive identity protection and credit monitoring service that would replace Equifax ID Patrol. The selection process included a detailed review of the products and services being offered, as well as extensive client reference checks, interviews and a site visit. InfoArmor and their product known as PrivacyArmor was selected for our faculty and staff. The University is providing this coverage at no cost to eligible faculty and staff, and coverage for eligible dependents may be selected during the upcoming Benefits Open Enrollment.

2. When does my InfoArmor coverage become effective?
   Your coverage is effective immediately.

3. What is included in my coverage through InfoArmor?
   PrivacyArmor’s coverage for Northwestern faculty and staff automatically includes the following services. You do not need to take any steps to receive:
   • $1,000,000 identity theft insurance policy
   • Privacy advocate remediation
   • Identity and credit monitoring
   • Compromised credentials monitoring
   • High risk transaction alerts
   • Financial transaction monitoring

   To provide more comprehensive identity protection, you may activate the following services on the InfoArmor website, also at no cost to you:
   • Credit scores and reports
   • Financial threshold monitoring
   • Social media reputation monitoring
   • Wallet protection
   • Digital exposure report
   • Solicitation reduction

4. How does InfoArmor protect my identity?
   By proactively monitoring for fraud, InfoArmor can quickly detect fraudulent activity. This coverage includes detecting fraud from sources such as wireless accounts, automobile and mortgage loans, compromised credentials, High Risk Transactions (such as unauthorized account access, fund transfers and password resets) and more. When suspicious activity is detected InfoArmor will alert you and help you restore your identity and minimize the impact of fraudulent activity.

5. How does InfoArmor prevent my identity from being misused?
   InfoArmor engages in proactive prevention to protect your identity from misuse. InfoArmor’s technology is predictive, meaning it is designed to detect when an identity is at an elevated risk for identity theft and take the necessary precautions. If you fall under this category, they will provide steps such as fraud alerts, credit freezes and pull credit reports to prevent fraud from occurring. Additionally, when fraud is detected, they know about it sooner than some other credit solutions because their technology detects fraud
at point of application rather than long after damage has been done. In addition, PrivacyArmor includes free credit monitoring, a monthly credit score and an annual credit report to protect your finances. Their system provides complete 360° protection to help deter, detect, and defend against identity theft.

6. Is it safe to give InfoArmor my personal information?
InfoArmor adheres to a comprehensive information security policy that applies to all employees, consultants, contractors and vendors that interact with InfoArmor and its information assets. Customer data is stored in a state-of-the-art data center (SSAE 16 Type II and DISA STIG compliant). That data is only accessible via secure, encrypted connections.

7. How does InfoArmor compare to other services, like credit monitoring?
InfoArmor detects a different type of identity theft that is not related to credit accounts. InfoArmor’s identity monitoring provides a broader range of protection by monitoring for misuse of not only credit, but also a variety of data sources. Credit is an important component in identity protection, but it represents a piece of the whole issue of identity protection. InfoArmor’s service includes (free of charge) an annual credit report, monthly credit scores and credit monitoring.

8. How do I know that my identity is secure?
InfoArmor sends monthly identity updates with your identity risk level and any active identity alerts. InfoArmor will alert you as soon as they detect an issue or suspicious activity via your communication preferences. You will be able to discuss next steps with an InfoArmor Privacy Advocate if suspicious activity is fraudulent.

9. How do I log in to view my account and turn on the additional features like CreditArmor, SocialArmor, and WalletArmor?
To securely access InfoArmor’s WebPortal, visit the Northwestern InfoArmor webpage. This page is securely located behind Northwestern’s single sign-on technology. From the Northwestern InfoArmor webpage, click on the “Create Your Profile with InfoArmor” button and follow these steps:

1. Enter your Northwestern email address for your username.
2. Enter your 7-digit Northwestern employee ID found on your Wildcard as your temporary password.
3. The system will immediately prompt you to change your temporary password by telling you that your password has expired. Select a new, unique password to use going forward. Confirm your new password. then hit "submit."
4. From there you will be asked to verify your identity by either receiving an email from InfoArmor to your Northwestern email account, or to use a PIN. As a first time user, you need to choose to have an email sent to your Northwestern email address. This will generate the email message. The message will contain a one time passcode. You will need to use this one time passcode in order to complete registration.
5. Enter the unique one time passcode sent to you via email.
6. Activate all of your features to get the highest level of protection. Once you have logged in, completely fill out your profile. You may also input additional information to activate features such as CreditArmor, SocialArmor, WalletArmor and Threshold Monitoring. Click on the corresponding tabs for each feature for more directions.
10. When I activate CreditArmor, will my credit score go down?
Activating CreditArmor will not negatively affect your credit. Since you are not applying for credit, a hard inquiry will not be placed on your file. Once activated you will receive credit monitoring, an annual credit report and monthly credit scores.

11. What should I do if my identity is stolen?
InfoArmor’s Privacy Advocates will work on your behalf to restore your identity from start to case completion. Privacy Advocates are Certified Identity Theft Risk Management Specialists (CITRMS®). They are experts in identity restoration and are committed to doing the work necessary to restore your identity.

12. Should I place a fraud alert on my credit bureau files?
InfoArmor only recommends the use of fraud alerts if you have a reason to believe that your identity has been compromised or the InfoArmor system shows that your identity is at a high risk of identity theft.

13. What is Internet Surveillance?
The Underground Internet, also referred to as the Deep Web, is a place for cyber criminals to illegally store and sell Personal Identifiable Information. Internet Surveillance scans the Underground Internet for your personal information. Internet Surveillance scours an ever-evolving complex of over 30,000 compromised machines, networks and web services identified by InfoArmor and leading cyber security firms.

Whether it is personal identifying information (i.e. name, address or Social Security number), a medical insurance card or an email address, it is designed to find breached data and alerts you.
14. What is a Digital Exposure report?
This interactive, easy-to-read report not only summarizes what a real-time deep Internet search finds out about you, but also offers you a Privacy Grade with tips to better secure your information. Digital Exposure goes far beyond a typical Internet search and highlights your exposure on the Internet.

15. What is covered under your Identity Theft Insurance Policy?
InfoArmor’s Identity Theft Insurance Policy protects against financial damages of identity theft such as associated costs, legal defense expenses and lost wages incurred as a result of resolving the fraud. For a copy of the full policy, please contact InfoArmor directly.

16. What if I currently reside in another country? Can I still enroll and receive protection?
One of the components of InfoArmor’s monitoring service is your social security number. If you are residing in another country and are a US citizen or are from a US territory, InfoArmor can monitor your information for instances of fraud. InfoArmor will still be able to alert you if they find suspicious activity associated with your identity or credit. InfoArmor is unable at this time to monitor for foreign bank accounts.

17. What happens if I no longer work at Northwestern? Will I still be covered?
If you leave Northwestern, you can keep your coverage. You will receive an email from InfoArmor to let you know that they have been notified of your job status change and that you may continue coverage by using a credit/debit/bank account.

18. What should I do if I have questions?
You are welcome to direct any questions to the InfoArmor Privacy Advocates. They are available 24 hours a day, 7 days a week to ensure that you have help when you need it. Privacy Advocates may be reached at 866-460-2406 or email clientservices@infoarmor.com. You may also contact the Northwestern Benefits Division at 847-491-7513 during normal business hours or benefits@northwestern.edu.

19. Can I enroll my spouse and/or dependents in this coverage?
At the upcoming open enrollment, you will have the opportunity to add family members for a low premium.

20. What if I don't want to have this coverage? Can I cancel it?
Yes, at any time you may cancel the coverage by calling the InfoArmor Privacy Advocates at 866-460-2406 or contacting the Northwestern Benefits Division at 847-491-7513 or benefits@northwestern.edu during normal business hours.