INFOARMOR®
EMPLOYEE BENEFIT SOLUTIONS

Legal Access Plans

IDENTITY THEFT PROTECTION | PROPOSAL

Benefit Summary: PrivacyArmor

- Identity Monitoring
- WalletArmor
- $25K ID Theft Insurance Policy
- Internet Surveillance
- Privacy Advocate Remediation
- Solicitation Reduction
- Digital Identity
- IdentityMD

Benefit Features:

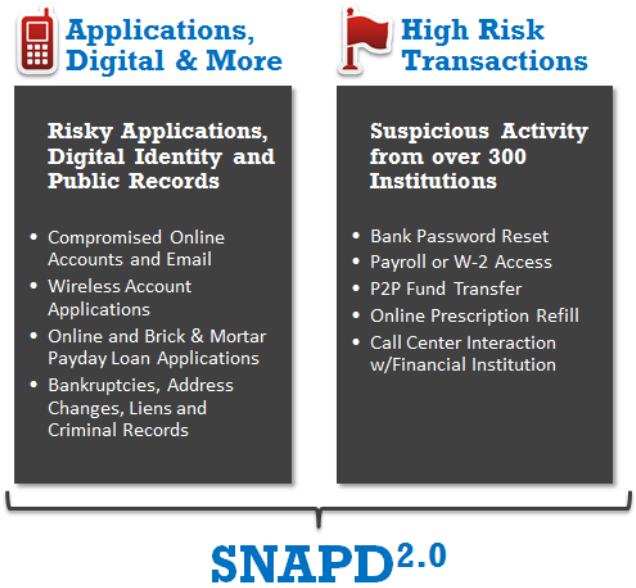
Identity Monitoring

Identity Monitoring is engineered to protect and engage consumers with unparalleled insight, actionable intelligence and early detection of financial fraud and privacy breaches. It uncovers security concerns at their inception so they can be resolved before major damage occurs.

SNAPD$^{2.0}$ Identity Monitoring offers consumers insight into everything from new loans to cellular phone applications to compromised online accounts. And now with the addition of industry-leading high risk transaction alerts, consumers will know when suspicious transactions occur with over 300 participating banks, online retailers, health insurers and more. Whether a fraudster succeeds or not, consumers are alerted when a bank password reset request is made, a new credit card is activated or access to their health insurance portal is attempted.

At InfoArmor, stopping more fraud faster is our goal and SNAPD$^{2.0}$ makes that a reality every day for hundreds of thousands of consumers.

PrivacyArmor can identify anomalies indicative of fraudulent activity sooner than and on a broader scope than competitors that rely solely on credit monitoring programs, because this identity monitoring program searches for fraud at the point of new account *application/creation* (vs. new account *approval*).



Internet Surveillance

InfoArmor Internet Surveillance continuously monitors the Underground Economy to uncover compromised, sensitive information. Whether it is personal identifying data or a medical insurance card, SNAPD Internet Surveillance finds breached data and alerts in real time.

Where Internet Surveillance Monitors:

- Malicious Command & Control Networks
- Black Market Forums
- Known Compromised Machines & Servers
- Phishing Networks
- Exploited Websites

How We Monitor:

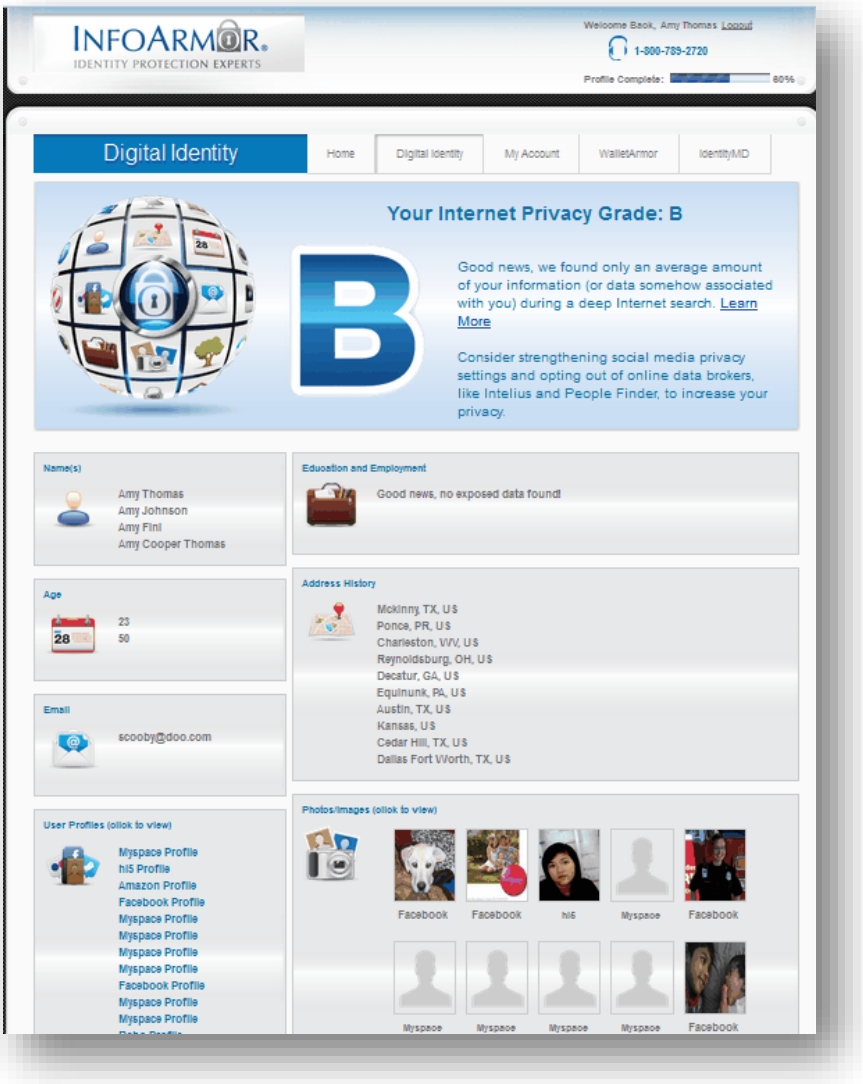
- Proprietary hardware and software solution
- Unparalleled alert accuracy (minimized false positives)
- Secure, separate reconnaissance and analysis efforts, plus no refined search queries

Data We Monitor:

- SSNs, names, addresses, emails and DOBs
- Wallet items (i.e. credit cards, medical insurance card)
- Login credentials including emails and passwords

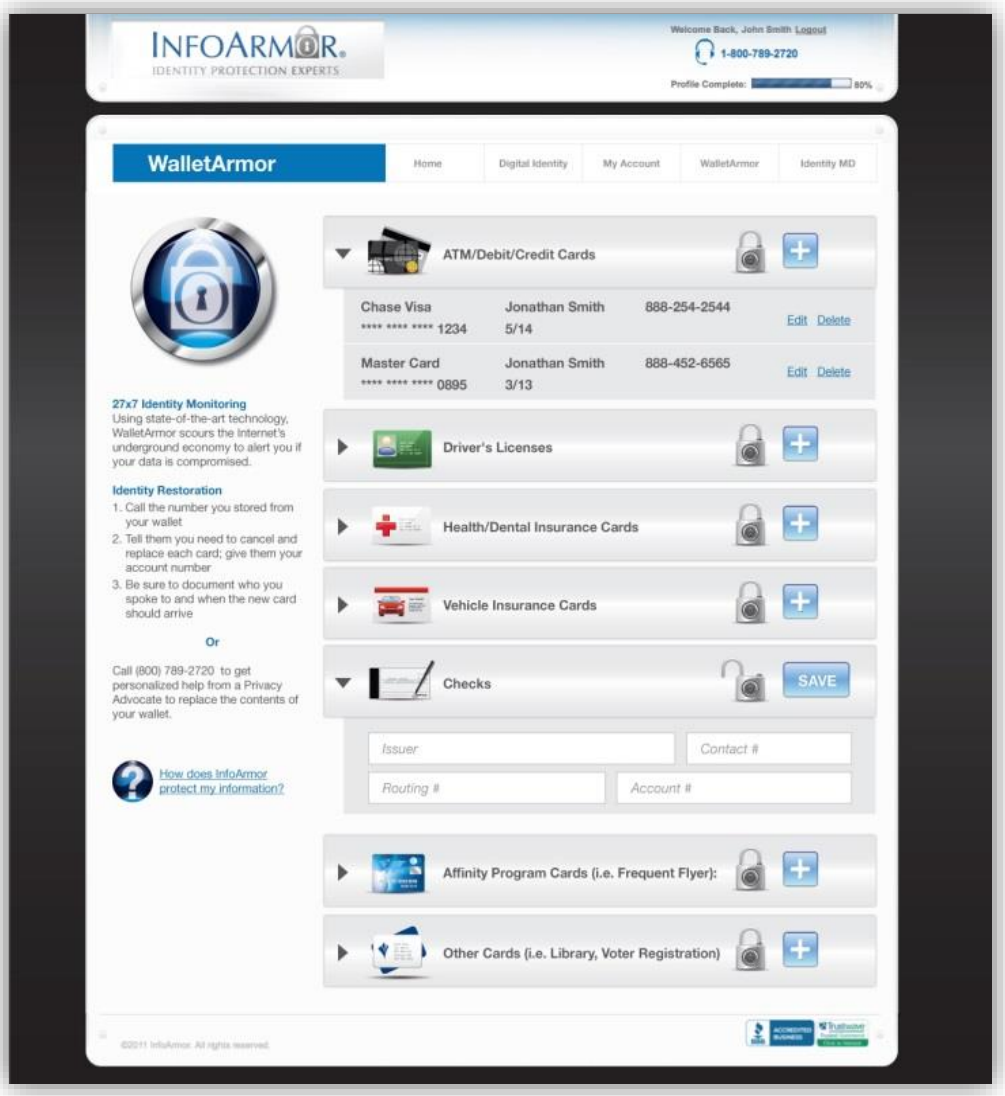
Digital Identity Report

This interactive, easy-to-read report not only summarizes what a deep Internet search uncovered, but also offers tangible value while InfoArmor monitors the Underground Economy.



WalletArmor

- 24x7x365 interactive monitoring to detect compromised credit cards, medical insurance identification, etc.
- Enhanced interface enables easy storage of important documents
- Expert Privacy Advocate aid in replacing lost/stolen wallets
- Alerting for expiration dates
- Categories include:
    - ATM, Debit, and Credit Cards
    - Driver's Licenses
    - Health and Dental Insurance Cards
    - Vehicle Insurance Cards
    - Checks
    - Affinity Cards (i.e. frequent flyer cards)
    - Miscellaneous Cards (i.e. Library and Voter Registration cards)



Full Service Privacy Advocate® Restoration

Upon notification of an identity theft incident, Privacy Advocates will immediately reach out to act on behalf of the victim as a dedicated case manager to:

- Investigate and, when appropriate, confirm fraudulent activity including known, unknown, and potentially complicated additional sources of identity theft.
- Complete and mail customized, pre-populated, state specific fraud packet via certified mail with pre-paid return instructions.
- Place phone calls, send electronic notifications, and prepare appropriate documentation on the victim's behalf, including anything from dispute letters to defensible complaints, to all appropriate agencies, financial institutions, etc.
- Issue fraud alerts and victim's statements when necessary, with the three consumer credit reporting agencies, the FTC, SSA, and U.S. Postal Service.
- Submit Special Limited Power of Attorney and ID Theft Affidavit to involved creditors for card cancellation and new card issuance.
- Contact, follow up and escalate issues with affected agencies, creditors, financial institutions, etc. to reinforce employee's rights.
- Assist the employee in notifying local authorities to file an official report(s).
- Utilize real time access to public records reports for further investigation where applicable.
- Provide peace of mind and resolution of key issues from start to finish as swiftly as possible.
- Provide copies of documentation, correspondence, forms and letters for the victim's personal records.

IdentityMD

IdentityMD is a resource to help individuals to prevent identity theft and manage the identity recovery process. It helps individuals remain in control of private information and thwart identity-related crimes before they happen. IdentityMD provides tips, tools, and resources to empower individuals to prevent identity theft and manage the identity recovery process if fraud occurs.

$25,000 Identity Theft Insurance Policy

Underwritten by AIG, the $25,000 Identity Theft Insurance policy provides reimbursement for out of pocket costs such as: lost wages, legal fees, notarizing fraud affidavits, certified mail, postage costs and long distance phone charges.

Privacy Advocates provide assistance with making a claim.

Online Account

Subscribers can login to their online account on a regular basis for the following features:

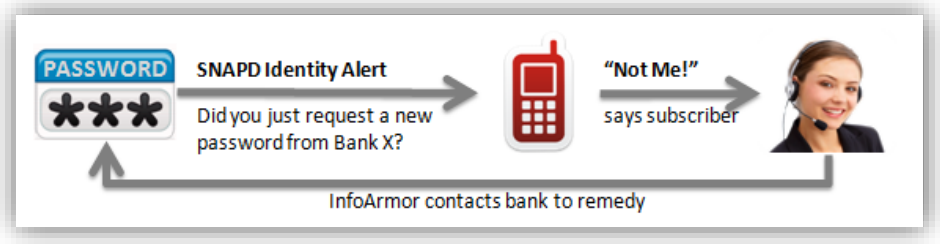
- Verify identity alerts and confirm or deny suspicious activity
- Activate credit monitoring and view free monthly credit scores and annual credit report
- Review Digital Identity report
- Protect wallet and/or purse contents using WalletArmor and receive alerts if information is detected on the Underground Internet
- Store passwords and login information for commonly used websites
- Update account information

Sample:
At 11:11 PM June 1, 2012 did you complete an online transaction with Bank X?

Subscriber Portal

Alerting Process:

InfoArmor proactively generates alerts via email, SMS/Text Message, or automated voice dialers to alert subscribers quickly when there is activity associated with their account. We strive to minimize false positives by implementing sophisticated algorithms based off of subscriber feedback to provide the most effective alerting procedures. If there is ever an *issue* that appears to be fraud a live Privacy Advocate will always reach out to the subscriber.



Solicitation Reduction

PrivacyArmor's solicitation opt out program enables employees to manage direct marketing campaigns from businesses or organizations in which they do not have (or want) an existing relationship. The service includes the ability (not requirement) to opt in or out of the following:

- Mail filtering
- Pre-approved credit and insurance offers
- National Do Not Call Registry
- Email solicitations

Reduction in these unwanted solicitations limits exposure of personal information, and therefore reduces the root cause of up to 20% of identity theft.

Differentiation:

Compared to other identity theft protection programs, PrivacyArmor catches:

More: Detection capabilities are more far reaching, as InfoArmor identity monitoring captures 79% more fraudulent activity than credit monitoring programs alone.

Sooner: Most of our competitors can only see new account information after the account activity has already occurred. Since credit-only programs can only detect theft after the account opening process has been completed and ultimately approved, they can only catch theft after the fact – once damages have occurred.

Retroactively: Components of InfoArmor's service can detect historical fraud, such as fraud that occurred before a subscriber enrolled in the solution. In the event we detect fraud, even a "pre-existing" case of fraud, InfoArmor's Privacy Advocates will provide full-service restoration to help fix the identity issue.

Even unsuccessful attempts at identity theft: Because InfoArmor seeks out theft at the application level, we can catch even the unsuccessful attempts. Other identity monitoring programs only see the accounts that are successfully created and opened. As a result, other programs cannot put the proper and appropriate safeguards in place before another attempt at theft is committed, whereas InfoArmor can and does.

Voluntary Payroll Deduction - $6.85 Composite Price per month

- All employees in the workplace population are covered with Full Service Privacy Advocate Restoration and $25,000 Identity Theft Insurance Policy
- Each employee on his/her own activates the proactive benefit features by sharing enrollment information with InfoArmor directly via web or phone – Identity Monitoring, access to portal features such as WalletArmor, Solicitation Reduction, Internet Surveillance, IdentityMD and Digital Identity.
- Even if no action taken by an employee, he/she would be covered by restoration services and reimbursement policy.
- Employee is covered immediately as of employer chosen effective date; employee enrolls additional family members via online account

INFOARMOR®
EMPLOYEE BENEFIT SOLUTIONS