Data breaches and identity theft in the public sector

Why is the public sector targeted?

- Government employees are targets for more than just identity thieves; they are also targets of organized crime groups and often fellow employees
- Criminals can use a government employee's personal data to access government databases and file fraudulent tax returns
- Scammers who obtain unlawful access to government data could also steal government benefits or gain restricted clearance
- In addition to being targeted by for-profit hackers, the public sector is also targeted by foreign governments for espionage

Must-know data breach statistics for the public sector

23,399 security incidents occurred in 2018[1]

330 confirmed data breaches occurred in 2018[1]

3M+ people's data records were exposed by public sector breaches[2]

75% of the data breaches came from external threats[1]

68% of the data exposed in public sector breaches in 2018 was internal[1]

66% of the breaches were motivated by espionage[1]

Take a closer look at some recent incidents

- In 2019, the Federal Emergency Management Agency (FEMA) experienced a security incident exposing the personal information of 2.3 million natural disaster victims[2]
- U.S. Customs and Border Protection experienced a third-party breach exposing a database of traveler personal data, including biometrics information[2]
- Over 320,000 records of individual payment details (and counting) have been exposed by Click2Gov, a government bill-pay portal compromised twice between 2017 and 2019[2]

Allstate SM
IDENTITY PROTECTION

Protect your employees, protect your business

Empower your employees with the protection they're looking for. High quality, valuable privacy protection improves public perception and trust. Plus, it may reduce the probability of litigation for your organization and increase your employees' security awareness and safety.

76% of Americans don't believe companies are doing their part to protect data[6]

50% of Americans say they don't know who to trust[5]

Why choose Allstate Identity Protection

Best-in-class technology, innovation and expertise

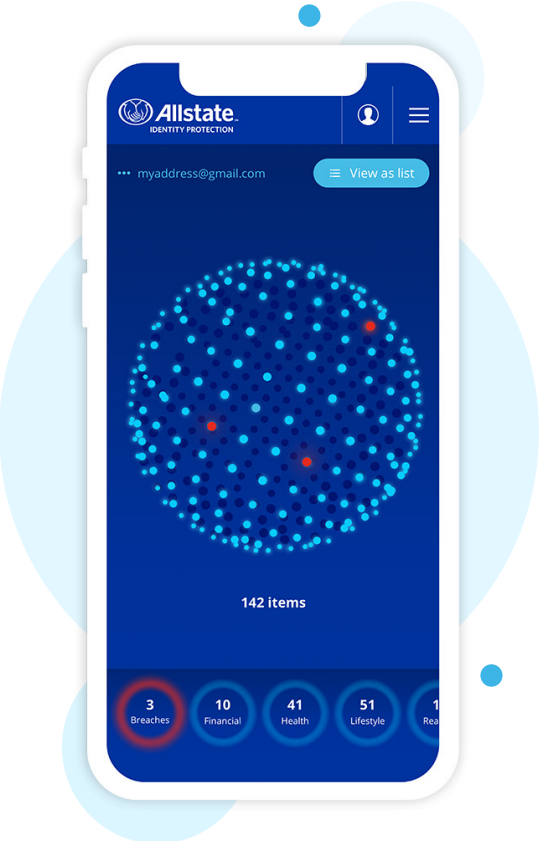
91.4
Net Promoter Score (NPS)

98%
implementation satisfaction rate

99%
account management satisfaction rate

99%
client retention

- Comprehensive and ongoing administrative support
- Easy onboarding that includes comprehensive product education and a dedicated client relationship advisor
- Scalable and flexible payment models that minimize risk
- Expert customer service representatives based in the U.S.
- Proactive, real-time alerts that help employees manage their privacy
- In-depth monitoring of the dark web for employees' compromised personal data, plus high risk transactions, data breach notifications, and more
- Tools to monitor and preserve an employee's reputation across social networks
- A dedicated advocate to guide and manage an employee's full recovery process



Ready to get started?

Contact us at sales@infoarmor.com

1 Verizon Enterprise, "2019 Data Breach Investigations Report," May 2019
2 Identity Theft Resource Center, "End-of-Year Data Breach Report," January 2020
3 Allstate Data Privacy and Consumer Expectations Survey
4 Allstate Digital Safety Offering Study, MARA

†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.

Allstate SM
IDENTITY PROTECTION