Data breaches and identity theft in the accounting industry

Why is the accounting industry targeted?

- Accounting firms and tax professionals store highly valuable data, which can include: client banking information, Social Security numbers, addresses, and other forms of personally identifiable information
- Cybercriminals stealing credentials could gain access to customer data or install malware on the firm's network
- Once cybercriminals access a firm's client records, they can then blackmail the firm with no guarantee they'll release the data upon ransom payment

Must-know data breach statistics for the accounting industry

670 security incidents occurred in 2018[1]

150 confirmed data breaches occurred in 2018[1]

5-7 data theft reports a week are sent to the IRS by tax practitioners[2]

$1.8B in various tax frauds were caught by the IRS in 2019[3]

What is tax fraud?

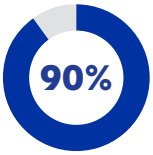
Tax fraud occurs in a variety of ways, but the most popular involves identity thieves stealing the personal information of a firm's clients and filing fraudulent tax returns on their behalf.

This is often accomplished via phishing.
Phishing (n.): A scam that occurs when cybercriminals send fraudulent emails to unsuspecting users or corporations in the hopes of stealing their personal information and private data. They request sensitive data from victims and then use that data for nefarious purposes, such as gaining access to customer records.

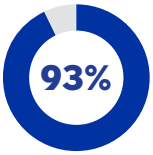
Accounting firms are huge targets for hackers

In 2019, cybercriminals launched a malware attack on Wolters Kluwer, a tax and accounting software platform used by:

100 **of the top U.S. accounting firms[4]**



of top global banks[4]



of Fortune 500 companies[4]

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

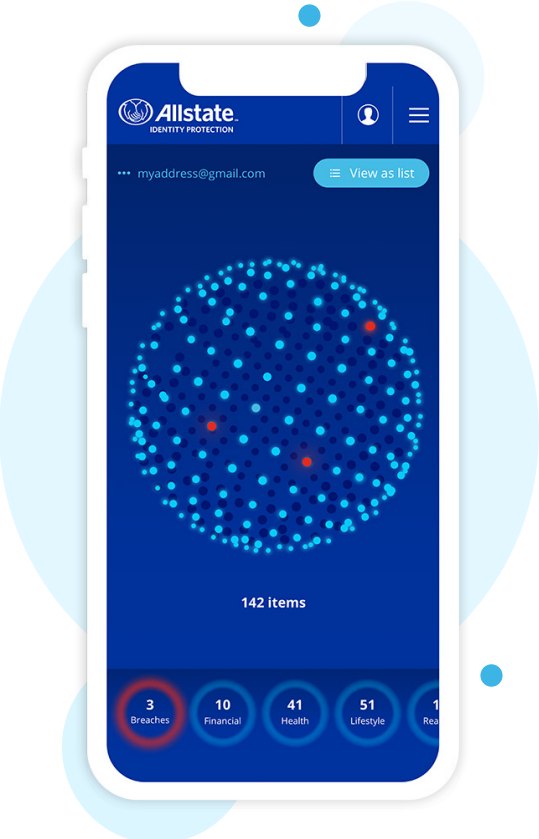
91.4
Net Promoter Score (NPS)

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 IRS, "IRS, Security Summit Partners warn tax professionals of high risk of data theft attacks," 2018
3 IRS Criminal Investigation Annual Report 2019
4 CNBC, "A malware attack against accounting software giant Wolters Kluwer is causing a 'quiet panic' at accounting firms," May 2019
5 Allstate Digital Safety Offering Study, MARA
6 Allstate Data Privacy and Consumer Expectations Survey
†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