March 2017

IDENTITY THEFT SERVICES

Services Offer Some Benefits but Are Limited in Preventing Fraud

GAO Highlights

Highlights of GAO-17-254, a report to congressional requesters

Why GAO Did This Study

Private-sector and government entities that experience data breaches often provide affected consumers with identity theft services, which typically include credit monitoring, identity monitoring, identity restoration, and identity theft insurance. In response to data breaches in 2015, OPM awarded two contracts obligating about $240 million for identity theft services.

GAO was asked to examine issues related to identity theft services and their usefulness. This report examines, among other objectives, (1) the potential benefits and limitations of identity theft services, and (2) factors that affect government and private-sector decision-making about them. GAO reviewed products, studies, laws, regulations, and federal guidance and contracts, and interviewed federal agencies, consumer groups, industry stakeholders, and eight providers selected because they were large market participants.

What GAO Recommends

Congress should consider permitting agencies to determine the appropriate coverage level for identity theft insurance they offer after data breaches. OMB should analyze the effectiveness of identity theft services relative to alternatives, and should explore options to address duplication in federal agencies' provision of these services. OPM should address in its breach-response policy when to offer these services and should document its decision-making process. OPM agreed with GAO's recommendations to the agency.

View GAO-17-254. For more information, contact Lawrance Evans at (202) 512-8678 or evansl@gao.gov.

What GAO Found

Identity theft services offer some benefits but have limitations.

- **Credit monitoring** helps detect new-account fraud (that is, the opening of new unauthorized accounts) by alerting users, but it does not prevent such fraud or address existing-account fraud, such as misuse of a stolen credit card number. Consumers have alternatives to credit monitoring, including requesting a low-cost credit freeze, which can prevent new-account fraud by restricting access to the consumers' credit report.
- **Identity monitoring** can alert consumers to misuse of certain personal information by monitoring sources such as public records or illicit websites, but its effectiveness in mitigating identity theft is unclear.
- **Identity restoration** seeks to remediate the effects of identity theft, but the level of service varies: some providers offer hands-on assistance, such as interacting with creditors on the consumer's behalf, while others largely provide self-help information, which is of more limited benefit.
- **Identity theft insurance** covers certain expenses related to the process of remediating identity theft but generally excludes direct financial losses, and the number and dollar amount of claims has been low.

These services also typically do not address some types of threats, such as medical identity or tax refund fraud.

Various factors affect government and private-sector decision making about offering identity theft services, and federal guidance related to these services could be improved. In the federal sector, legislation requires certain agencies to provide identity theft services. For example, legislation requires the Office of Personnel Management (OPM) to provide these services to individuals affected by its 2015 data breaches for 10 years, as well as provide $5 million in identity theft insurance. However, this level of insurance coverage is likely unnecessary because claims paid rarely exceed a few thousand dollars. Requirements such as this could serve to increase federal costs unnecessarily, mislead consumers about the benefit of such insurance coverage, and create unwarranted escalation of coverage amounts in the marketplace. The Office of Management and Budget (OMB) has guidance on agencies' response to data breaches, but this guidance does not address the effectiveness of these services relative to lower-cost alternatives, in keeping with OMB's risk management and internal control guidance. Further, OPM provided duplicative identity theft services for about 3.6 million people affected by both of its 2015 breaches, and OMB has not explored options to help federal agencies avoid potentially wasteful duplication. In addition, contrary to key operational practices previously identified by GAO, OPM's data-breach-response policy does not include criteria or procedures for determining when to offer identity theft services, and OPM has not always documented how it chose to offer them in response to past breaches, which could hinder informed decision making in the future. In the private sector, companies often offer consumers affected by a data breach complimentary identity theft services for reasons other than mitigating the risk of identity theft, such as avoiding liability or complying with state law.