March 2019

GAO Highlights

Highlights of GAO-19-230, a report to congressional requesters

DATA BREACHES

Range of Consumer Risks Highlights Limitations of Identity Theft Services

Why GAO Did This Study

Recent large-scale data breaches of public and private entities have put hundreds of millions of people at risk of identity theft or other harm. GAO was asked to review issues related to consumers' options to address risks of harm from data breaches. This report, among other things, examines information and expert views on the effectiveness of consumer options to address data breach risks. GAO analyzed available data on options, collected and analyzed related documentation, conducted a literature review of studies, and interviewed a nongeneralizable sample of 35 experts (from academia, government entities, consumer and industry organizations) and identity theft service providers to reflect a range of views.

What GAO Recommends

GAO reiterates a matter for congressional consideration and a recommendation from its 2017 report on identity theft services (GAO-17-254). In that report, GAO found that legislation requiring federal agencies that experience data breaches, including OPM, to offer certain levels of identity theft insurance coverage to affected individuals requires coverage levels that are likely unnecessary. Therefore, Congress should consider permitting agencies to determine the appropriate coverage level for such insurance. GAO also recommended the Office of Management and Budget (OMB) update its guidance for agency responses to data breaches, after analyzing the effectiveness of identity theft services relative to lower-cost alternatives. OMB did not agree or disagree and had not taken action as of early March 2019.

View GAO-19-230. For more information, contact Anna Maria Ortiz at (202) 512-8678 or ortiza@gao.gov.

What GAO Found

No one solution can address the range of potential risks from a data breach, according to interviews with academic, consumer, government, and industry experts and documentation GAO reviewed. Perpetrators of fraud can use stolen personal information—such as account numbers, passwords, or Social Security numbers—to take out loans or seek medical care under someone else's name, or make unauthorized purchases on credit cards, among other crimes. Foreign state-based actors can use personal information to support espionage or other nefarious uses.

Public and private entities that experience a breach sometimes provide complimentary commercial identity theft services to affected individuals to help monitor their credit accounts or restore their identities in cases of identity theft, among other features. Consumers also may purchase the services. As of November 30, 2018, the Office of Personnel Management (OPM) had obligated about $421 million for a suite of credit and identity monitoring, insurance, and identity restoration services to offer to the approximately 22 million individuals affected by its 2015 data breaches. As of September 30, 2018, about 3 million had used the services and approximately 61 individuals had received payouts from insurance claims, for an average of $1,800 per claim. OPM re-competed and awarded a contract to the previously contracted company in December 2018.

GAO's review did not identify any studies that analyzed whether consumers who sign up for or purchase identity theft services were less subject to identity theft or detected financial or other fraud more or less quickly than those who monitored their own accounts for free. A few experts said consumers could sign up for such services if offered for free. Credit monitoring may be convenient for consumers and personalized restoration services may help identity theft victims recover their identities, but such services do not prevent fraud from happening in the first place. The services also do not prevent or directly address risks of nonfinancial harm such as medical identity theft.

Consumer, government, and industry experts highlighted other free options, including a credit freeze, which prevents one type of fraud. A freeze restricts businesses from accessing a person's credit report—and can prevent the illicit opening of a new account or loan in the person's name. A provision of federal law that took effect in September 2018 made it free for consumers to place or lift credit freezes quickly at the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion). Consumers also can regularly monitor their accounts and review their credit reports for free every 12 months. In addition, they can take advantage of free federal assistance such as the guidance on the Federal Trade Commission's IdentityTheft.gov website.

Finally, large amounts of personal information are outside of consumers' control and bad actors can use stolen information for years after a breach. Therefore, experts noted that data security at entities that hold such information—and efforts to make stolen information less useful for identity thieves, through use of new identity verification technologies, for example—are important ways to mitigate risks of harm for consumers.