GAO Highlights

RETIREMENT PLANS

Department of Labor Guidance Could Mitigate Privacy Risks for Participants

GAO-26-107271 February 2026

A report to congressional requesters

For more information, contact: Tranchau (Kris) Nguyen at nguyentt@gao.gov or Marisol Cruz Cain at cruzcainm@gao.gov

What GAO Found

Retirement plan sponsors, typically a person's employer, share participant information, including personally identifiable information (PII), with service providers, such as asset managers and record keepers, who help administer the plan. However, these providers may also use PII and other information to market financial products and services or, in some cases, sell this information, according to GAO's review of 31 service provider privacy disclosures (see figure). As more entities gain access to participant data, the chance that their information may be inadvertently exposed increases, putting participants at greater risk of identity theft or other fraudulent activity. Service providers that GAO interviewed noted, however, that greater use and sharing of participant information helped them to more effectively target products and services that might benefit participants.

31 Retirement Plan Service Provider Policies on Sharing or Selling Participant Data

Source: GAO analysis of selected retirement plan service provider privacy disclosures. | GAO-26-107271

Selected service provider privacy disclosures that GAO reviewed did not consistently incorporate leading privacy practices. Fair Information Practice Principles emphasize key data privacy protection principles, such as transparency in data practices and restrictions to prevent unauthorized uses of personal information. All 31 disclosures described their policies for the collection and use of personal information, in alignment with the principle related to transparency. However, many of the disclosures did not fully align with other principles. For instance, most disclosures (19 of 31) did not indicate that additional consent would be sought before sharing or otherwise using personal information beyond originally specified purposes, contrary to the principle related to use limitation.

Federal agencies and states have taken some steps to protect consumer data privacy, but the Department of Labor (DOL) has not taken actions against retirement plans for sharing participant data. The Employee Retirement Income Security Act of 1974, as amended (ERISA) does not address data privacy explicitly, but DOL officials said that the agency believes that ERISA's duties of prudence and loyalty should sufficiently deter plan sponsors and service providers from unauthorized uses of participant data. In addition, DOL issued cybersecurity guidance in April 2021 that discussed data privacy as a component of cybersecurity. However, DOL's guidance does not include detailed information about good practices for sharing data about plan participants. Additional guidance would better position plan sponsors and service providers to understand acceptable uses of participant data and the circumstances in which they should obtain permission to use or disclose information about participants, particularly given potentially differing state requirements.

Why GAO Did This Study

About 126 million Americans participated in defined contribution retirement plans, with assets totaling over $9 trillion, as of 2023 (most recent data). As the number of participants and the volume of assets grow, so too does the importance of ensuring responsible handling of participants' data. However, participants have filed several lawsuits alleging that service providers used their data for targeted marketing.

GAO was asked to review retirement plan data privacy. This report examines (1) how selected retirement plans use and share participant data, (2) how selected service provider policies incorporate leading privacy practices, and (3) how federal agencies and selected states protect consumer data privacy as it applies to retirement plans.

GAO assessed publicly available privacy disclosures from a nongeneralizable sample of 31 service providers selected based on size, among other factors. GAO identified the extent to which selected disclosures allowed participant data to be shared or sold for targeted marketing and compared the disclosures to recognized data privacy guidance. GAO also reviewed privacy disclosures from six selected plan sponsors. GAO reviewed relevant federal laws and regulations and interviewed officials from DOL and other federal agencies, among others. GAO also assessed state privacy laws and obtained information from officials in three selected states on the laws' applicability to retirement plans.

What GAO Recommends

GAO is recommending that DOL provide additional guidance about participant data privacy for retirement plan sponsors and service providers. DOL neither agreed nor disagreed with the recommendation, as discussed in the report.