United States Government Accountability Office

Report to Congressional Requesters

February 2026

RETIREMENT PLANS

Department of Labor Guidance Could Mitigate Privacy Risks for Participants

GAO-26-107271

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.

Contents

Tables

Figures

Abbreviations

CFPB	Consumer Financial Protection Bureau
DB	defined benefit
DC	defined contribution
DCIIA	Defined Contribution Institutional Investment Association
DOL	Department of Labor
EBSA	Employee Benefits Security Administration
ERISA	Employee Retirement Income Security Act of 1974, as amended
FCRA	Fair Credit Reporting Act
FIPP	Fair Information Practice Principles
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
OECD	Organisation for Economic Co-operation and Development
PII	personally identifiable information
SEC	Securities and Exchange Commission
SPARK	Society of Professional Asset Managers and Recordkeepers

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

February 26, 2026

The Honorable Bernard Sanders
Ranking Member
Committee on Health, Education, Labor and Pensions
United States Senate

The Honorable Robert C. “Bobby” Scott
Ranking Member
Committee on Education and Workforce
House of Representatives

The Honorable Patty Murray
United States Senate

Tens of millions of Americans participate in defined contribution (DC) retirement plans, such as 401(k) and 403(b) plans, as a primary means of preparing for retirement. DC plans are individual account-based plans where participants contribute a portion of their earnings, sometimes matched by employers, and invest in a choice of assets. To administer and service these plans, plan sponsors, often a person’s employer, typically share participants’ personal and financial data with one or more service providers.[1] However, sharing participants’ data introduces potential privacy risks as more entities gain access to participant data. In addition, some providers may use participant data for secondary purposes, such as targeted marketing or selling to data brokers and other third parties.[2]

According to the Department of Labor (DOL), more than 126 million Americans participated in DC private-sector retirement plans as of 2023, the most recent data available, with assets totaling over $9 trillion.[3] As the number of participants and the volume of assets continue to grow, so

[1]Service providers are entities such as record keepers or asset managers that retirement plan sponsors hire to help administer a defined contribution retirement plan.

[2]Data broker refers to a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

[3]Department of Labor, Employee Benefits Security Administration, *Private Pension Bulletin, Abstract of 2023 Form 5500 Annual Reports* (Washington, D.C.: Sept. 2025).

does the importance of ensuring responsible handling of retirement plan participant data.

The Employee Retirement Income Security Act of 1974, as amended (ERISA) establishes foundational protections for retirement plan participants, but it does not directly address data privacy in the modern digital age. In practice, many plan sponsors rely on a complex web of service providers, each of which may have its own standards and policies regarding data usage. Accordingly, participants may not always be aware of how their information is being collected, used, and potentially shared.

You asked us to examine how data on retirement plan participants is used and shared by service providers, including whether such data is used beyond purposes of plan administration and potentially shared with third parties. This report examines: (1) how retirement plan service providers and sponsors use and share participant data and the potential benefits and risks of current data sharing practices, (2) how selected retirement plan service provider policies incorporate leading practices for data privacy, and (3) how federal agencies and selected states oversee consumer data privacy as it applies to retirement plans.

To assess how retirement plan service providers use and share participant data, we reviewed a nongeneralizable sample of publicly available privacy disclosures. Specifically, we reviewed publicly available privacy disclosures from 21 record keepers and 10 asset managers for a total of 31.[4] We reviewed each of these disclosures to identify the types of data being collected, the stated sources of this information (e.g., credit reporting agencies, social media, or other third-party sources), and the extent to which record keepers and asset managers stated that they used, shared, or sold participant data for targeted marketing. To identify record keepers, we consulted with an industry group and used their membership list as a basis for our sample. To identify asset managers, we used a retirement industry publication that provides institutional investment data and analysis on service providers.[5] We selected the ten largest asset managers by the amount of institutional assets invested as

[4]The findings from our review of selected privacy disclosures are not generalizable and cannot be used to make inferences about the entire population of record keepers or asset managers.

[5]"The Largest Money Managers 2023," *Pensions and Investments*, June 12, 2023.

of December 31, 2022, the most recent data available. For additional information about our methodology, see appendix I.

In addition, we reviewed publicly available privacy disclosures from six selected retirement plan sponsors.[6] We reviewed these disclosures to identify what, if any, limitations these sponsors placed on service providers, like record keepers and asset managers, about how they could use, share, or sell participant data. To identify plan sponsors, we used a retirement industry publication that provides institutional investment data and analysis on plan sponsors.[7] We initially selected the 10 largest defined contribution retirement plan sponsors by the amount of retirement assets invested as of September 30, 2022, the most recent data available. However, only six of the 10 selected plan sponsors had publicly available privacy disclosures available that were employee specific.[8] Therefore, we excluded the remaining four from review.

To understand the benefits and risks of current data sharing practices, we interviewed or obtained information from a total of 26 stakeholders, which included retirement industry associations, researchers, plan sponsors, record keepers, attorneys specializing in ERISA or data privacy, retirement plan consultants, and groups that advocate on behalf of retired people.[9] We also interviewed officials from data privacy groups and met with officials from DOL, which oversees retirement plans and benefits, as well as other federal agencies involved in overseeing consumer data privacy laws, including the Consumer Financial Protection Bureau

[6]The findings from our review of selected privacy disclosures are not generalizable and cannot be used to make inferences about the entire population of plan sponsors.

[7]"Largest U.S. Retirement Plans 2023," *Pensions and Investments*, Feb. 13, 2023.

[8]For plan sponsors, our review focused on employee specific privacy disclosures instead of customer specific disclosures aimed at those who may do business with the company or purchase its products or services.

[9]To identify relevant retirement stakeholders, we began by interviewing individuals, groups, and organizations that participated in a prior related GAO review. See GAO, *Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans,* GAO-21-25 (Washington, D.C.: Feb. 2021). During these interviews, we asked stakeholders to recommend other relevant individuals, groups, or organizations that we should contact to discuss how retirement plan sponsors and service providers use and share data about plan participants, as well as those that focus on consumer data privacy more generally. The interviews that we conducted are not generalizable and cannot be used to make inferences beyond the individuals, groups, or organizations that participated in our review.

(CFPB), Securities and Exchange Commission (SEC), and Federal Trade Commission (FTC).

To assess how selected retirement plan service provider privacy disclosures incorporate leading practices for data privacy, we used the Fair Information Practice Principles (FIPP), which are a set of high-level internationally recognized privacy protection principles.[10] To conduct our assessment, we reviewed the contents of publicly available privacy disclosures for 31 selected record keepers and asset managers to identify key elements related to consumer privacy protection. We then determined the extent to which the identified practices were in alignment with the relevant FIPPs. Specifically, we assessed the extent to which the selected disclosures fully incorporated, partially incorporated, or did not incorporate each of the eight FIPPs.[11]

To determine how federal agencies and selected states protect consumer data privacy in ways that might apply to retirement plans, we reviewed relevant federal laws and regulations, including ERISA and the Gramm-Leach-Bliley Act (GLBA), among others.[12] We also interviewed federal officials from DOL, CFPB, SEC, and FTC to discuss their oversight and enforcement of relevant federal law and regulations with respect to retirement plan sponsors and service providers. Further, to provide examples of complaints participants have alleged about the sharing of their personal information by plan sponsors or service providers, we identified and reviewed cases filed in federal courts that specifically included an allegation that a plan sponsor or service provider had used plan data without consent for targeted marketing. While not generalizable,

[10]These principles were first proposed in 1973 by a U.S. government advisory committee. In response to concerns about the potential consequences that computerized data systems could have on the privacy of personal information, the committee examined the extent to which limitations should be placed on using computer technology for record keeping about people. The Organisation for Economic Co-operation and Development (OECD) developed a revised version of the principles in 1980 that has been widely adopted. OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

[11]For additional information on our analysis of selected retirement plan service provider privacy disclosures see app. I.

[12]Enacted in 1999, GLBA governs the disclosure of nonpublic personal information that a financial institution maintains in connection with providing financial products and services to consumers.

reviewing these cases also allowed us to provide examples of actions plan sponsors have taken to address such allegations as part of settlement agreements reached between parties. Further, we reviewed DOL's cybersecurity guidance issued in 2021 for retirement plan sponsors and service providers to understand the extent to which data privacy was included as a component of cybersecurity.[13] We also assessed the clarity of DOL's cybersecurity guidance in relation to relevant federal internal control standards for information and communication.[14]

To understand consumer-oriented data privacy laws that have been enacted in various states, we reviewed research from IAPP and interviewed IAPP officials.[15] To complement our review of existing research, we also interviewed or obtained information from officials in three selected states—California, Colorado, and Virginia— to discuss how their state privacy laws may apply to retirement plans. We selected these states because their data privacy laws have been in effect the longest.

We conducted this performance audit from January 2024 to February 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[13]DOL updated its cybersecurity guidance in September 2024 to clarify that it applies to all plans covered by ERISA, including health plans and all employee retirement benefit plans.

[14]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 2014).

[15]IAPP is a not-for-profit organization and accredited certification body that publishes research on state level privacy legislation. It also assists companies and institutions in managing and protecting data, provides a forum for privacy professionals to share best practices, and track trends, among other things. IAPP, *US State Comprehensive Privacy Laws Report, 2023 Legislative Session* (Portsmouth, NH: Jan. 2024) and IAPP, *US State Privacy Legislation Tracker* (Portsmouth, NH: Nov. 24, 2025).

Background

Retirement plans are a critical financial resource for millions of Americans, providing long-term savings and investment opportunities to help individuals prepare for retirement. In the United States, private-sector employer-sponsored retirement plans fall into two main categories: defined benefit (DB) plans and defined contribution (DC) plans.[16] This report focuses on DC plans, which are employer-sponsored, account-based retirement savings plans. The most well-known type of DC plan is the 401(k) plan, which allows employees to contribute a portion of their earnings on a tax-advantaged basis, often with employer-matching contributions. These plans enable individuals to save and accumulate interest to build retirement savings over time.

Managing Retirement Plan Data

Administering retirement plans requires the collection, use, and sharing of participant data, with multiple entities assuming distinct roles and responsibilities. Among these entities, plan sponsors play a central role by maintaining the plan and generally serving as fiduciaries, which involves exercising authority over the plan's management. As we reported in 2021, plan sponsors share personally identifiable information (PII) on participants in the plan with service providers that help to administer the plan.[17] Service providers can include record keepers, asset managers, and payroll providers (see table 1).

Table 1: Examples of Defined Contribution Retirement Plan Service Providers

Service provider	Examples of service provider activities
Record keepers	Manage participant accounts, process contributions and distributions, maintain plan records, and provide online platforms for participants to access and manage retirement savings
Asset managers	Invest participant and employer contributions, offer a diverse selection of investment options to help participants grow their retirement savings
Payroll providers	Facilitate the transmission of payroll data, ensure that employee salaries and retirement contributions are accurately processed and delivered to record keepers for proper allocation

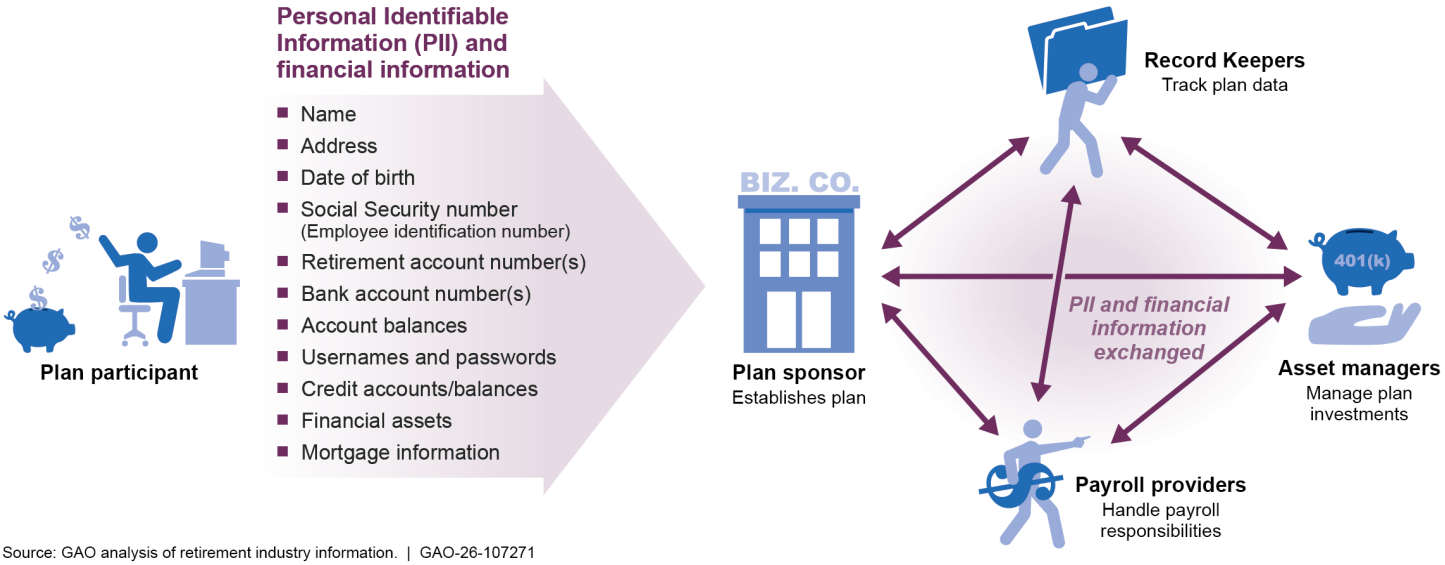
Source: GAO review of plan information. | GAO-26-107271

[16]A DB plan is an employer-sponsored retirement plan that traditionally promises to provide a fixed benefit for the life of the participant. The benefit amount is determined by a formula specified in the plan, which typically considers factors such as the employee's salary, years of service, and age at retirement.

[17]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number; and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information. GAO-21-25.

Some service providers may perform multiple roles within a retirement plan, such as acting as both the record keeper and the asset manager.[18] Figure 1 illustrates how PII and other financial information flows between plan sponsors and selected service providers for plan administration.

Figure 1: Data Sharing Among Plan Sponsors and Selected Service Providers in the Administration of Defined Contribution Retirement Plans



Source: GAO analysis of retirement industry information. | GAO-26-107271

ERISA

ERISA is the primary federal law governing most private sector employer-sponsored retirement plans in the United States. Established to protect plan participants and beneficiaries, ERISA sets minimum standards and requirements including those related to reporting and disclosure and fiduciary responsibilities. For instance, ERISA requires fiduciaries to carry out their duties with care and act solely in the interest of plan participants and beneficiaries. Plan fiduciaries can include plan sponsors and service providers, among others, depending on the functions they perform.

[18]We have reported previously that conflicts of interest are a common part of many financial transactions involving products recommended to retirement plan participants. Large firms with multiple lines of business and various affiliates can create potential conflicts. Federal law generally requires fiduciaries or service providers to avoid a transaction that places them in a conflicted position or constitutes a non-exempt prohibited transaction. However, despite obligations to mitigate and eliminate certain conflicts, conflicts of interest persist and can negatively impact plan participants. To better protect investors, we made two recommendations to IRS regarding oversight of prohibited transactions. The agency agreed with these recommendations. For more information, see GAO, *Retirement Investments: Agencies Can Better Oversee Conflicts of Interest between Fiduciaries and Investors*, GAO-24-104632 (Washington, D.C.: July 2024).

ERISA also prohibits certain transactions to help safeguard retirement plan assets from self-dealing, conflicts of interest, or other misuse.

While ERISA establishes responsibilities for plan fiduciaries (e.g., plan sponsors and certain service providers), it does not include explicit provisions addressing data privacy in retirement plans.[19] ERISA requires that plan fiduciaries use plan assets exclusively to provide plan benefits or to defray certain administrative costs. Some plan participants have argued that participant data should be considered a plan asset under ERISA, and that plan service providers that exercise authority and control over the management and disposition of participant data should be subject to ERISA's fiduciary responsibilities.[20] Courts that have ruled on this question, however, have rejected the argument that participant data should be considered a plan asset.[21]

The Employee Benefits Security Administration (EBSA) has primary responsibility within DOL for overseeing employer-sponsored retirement and group health plans under Title I of ERISA. EBSA administers and enforces the fiduciary, reporting, and disclosure provisions of Title I, working to ensure that plan participants receive their health and retirement benefits. EBSA is also responsible for interpreting ERISA and developing relevant regulations as well as developing the enforcement guidance regional office staff use to address inquiries and conduct investigations.

In February 2021, we made two recommendations to DOL to help clarify fiduciary responsibilities with respect to retirement plan cybersecurity and

[19]Although ERISA does not contain explicit provisions addressing data privacy, DOL regulations address data privacy in certain circumstances, according to DOL officials. For instance, to meet regulatory requirements when sharing documents electronically, plan administrators are required to take appropriate and necessary measures to protect the confidentiality of personal information relating to the individual's accounts and benefits. 29 C.F.R. § 2520.104b-1(c)(1)(i)(B).

[20]See, for example, *Harmon v. Shell Oil Co*., No. 3:20-cv-00021, 2021 U.S. Dist. LEXIS 66312 (S.D. Tex. Mar. 30, 2021).

[21]See, for example, id (granting a motion to dismiss where plaintiffs failed to cite any court that had ever held that releasing or allowing someone to use confidential information constituted a breach of fiduciary duty under ERISA); *Divane v. Northwestern. Univ.,* No. 16 C 8157, 2018 U.S. Dist. LEXIS 87645, at *38 (N.D. Ill. May 25, 2018) ("Plaintiffs cite no case in which a court has held that such information is a plan asset for purposes of ERISA. This Court does not intend to be the first.").

to provide guidance on cybersecurity risk mitigation.[22] In April 2021, EBSA issued cybersecurity guidance to plan fiduciaries highlighting the importance of securing plan data.[23] The guidance stated that plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks. EBSA prepared cybersecurity best practices for recordkeepers and other service providers responsible for plan-related information systems and data. EBSA also provided best practices for hiring service providers for plan fiduciaries.[24]

Consumer Data Privacy

As we have reported previously, the United States does not have a comprehensive federal privacy law that governs the collection, use, and disclosure of personal information by private sector entities, including those that administer retirement plans.[25] Instead, federal laws addressing privacy issues in the private sector are generally narrowly tailored to specific purposes, situations, types of information, or sectors or entities—such as data related to eligibility for credit, financial transactions, and personal health. For example:

- The Fair Credit Reporting Act (FCRA) protects the security and confidentiality of personal information collected or used to help make decisions about individuals' eligibility for credit, insurance, or employment. It provides consumers the right to opt out of consumer reporting agencies sharing their personal information with third parties for prescreened marketing offers.
- The Gramm-Leach-Bliley Act (GLBA) restricts sharing and disclosure of nonpublic personal information by financial institutions. For example, a third party that receives nonpublic personal information from a financial institution to process

[22]GAO-21-25. DOL neither agreed nor disagreed with the recommendation that the Secretary of Labor formally state whether cybersecurity is a fiduciary responsibility for private sector defined contribution retirement plans under ERISA. The agency stated in response that plan fiduciaries were required to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise.

[23]DOL updated its cybersecurity guidance in September 2024 to clarify that it applies to all plans covered by ERISA, including health plans and all employee retirement benefit plans.

[24]DOL's actions on cybersecurity guidance partially addressed GAO's second recommendation. To fully implement it, DOL should define a minimum set of expectations for mitigating cybersecurity risks in retirement plans and specific actions plan administrators and fiduciaries would be responsible for implementing to protect their systems and data.

[25]GAO, *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps,* GAO-19-621T (Washington, D.C.: June 2019).

consumers' account transactions may not use the information or resell it for marketing purposes.[26]

- The Health Insurance Portability and Accountability Act (HIPAA) establishes a set of national standards to protect certain health information. The HIPAA privacy rule governs the use and disclosure of an individual's health information for purposes including marketing.[27] With some exceptions, the rule requires an individual's written authorization before a covered entity—a health care provider that transmits health information electronically in connection with covered transactions, health care clearinghouse, or health plan—may use or disclose the information for marketing.

These laws are enforced by various federal agencies including CFPB, SEC, FTC, and the Department of Health and Human Services, depending on the type of entity or the specific facts and circumstances involved.

In September 2013, we recommended that the Congress consider strengthening the consumer privacy framework to reflect the effects of changes in technology and the marketplace—particularly in relation to consumer data used for marketing purposes—while also ensuring that any limitations on data collection and sharing do not unduly inhibit the economic and other benefits to industry and consumers that data sharing can accord.[28] We have continued to emphasize the need for stronger

[26]Nonpublic personal information can include information provided by a consumer when applying for credit—such as the consumer's Social Security Number, annual income, or outstanding debt—or which a financial institution otherwise collects or maintains in connection with providing a financial product or service to a consumer—such as the consumer's account balance, payment history, and credit card transactions.

[27]Individually identifiable health information is information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual; and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

[28]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace,* GAO-13-663 (Washington, D.C.: Sept. 2013).

consumer privacy protections in our High-Risk series over the years, particularly given changing technology.[29]

Several states have enacted privacy laws in recent years aimed at expanding protections for personal data. For example, in 2018, California became the first state to pass consumer-oriented data privacy legislation. As of November 2025, 19 states have enacted privacy laws that have already taken effect or that will do so in 2026.[30] In contrast to federal laws, which are typically sector-specific and apply to particular types of data, state privacy laws generally impose requirements, with certain exceptions, on a broad range of entities across various industries.[31] These laws often include provisions granting consumers rights over their personal data, obligations for transparency, and requirements for data security.

Leading Practices for Privacy Protections for Personal Information

The Fair Information Practice Principles (FIPP) are a set of internationally recognized principles for protecting the privacy and security of personal information. With some variation, the FIPPs have been widely used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States.[32] While FIPPs are principles as opposed to legal requirements, they provide a framework for balancing the need for privacy with other interests.

Table 2 describes the eight individual principles that constitute the FIPPs.

[29]GAO, *High Risk Series, Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* GAO-25-107743 (Washington, D.C.: Feb. 2025) and GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 2024).

[30]IAPP, *US State Privacy Legislation Tracker*.

[31]While these state laws generally apply broadly across various industries, certain categories of data already regulated under federal laws, such as health or financial information, and certain types of entities, such as nonprofit organizations and government agencies, may be exempt, according to IAPP. IAPP, *US State Comprehensive Privacy Laws Report, 2023* and IAPP, *US State Privacy Legislation Tracker*.

[32]The FIPPs served as the basis for the Privacy Act of 1974, which governs the collection, maintenance, use, and dissemination of personal information by federal agencies.

Table 2: Fair Information Practice Principles (FIPP)

Principle	Description
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

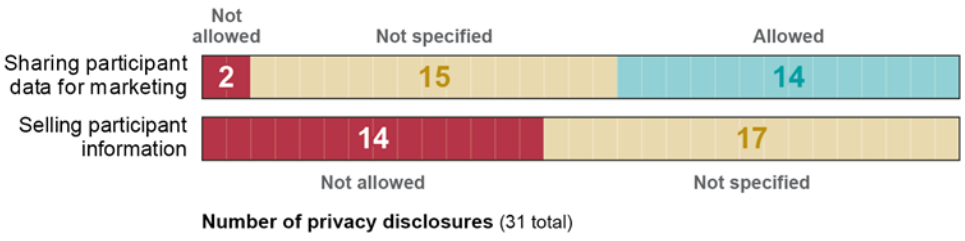
Source: Organisation for Economic Co-operation and Development. | GAO-26-107271

Retirement Plans Use and Share Participant Data to Administer Plans, but Selected Service Providers May Share or Sell Data, Increasing Privacy Risks

Plan Sponsors Collect and Share Participant Data, but Most Selected Privacy Disclosures Do Not Limit the Service Providers' Ability to Share or Sell Participant Data

Retirement plans rely on participant data to ensure accurate plan administration. Plan sponsors share participant PII and financial information with service providers so that the providers can perform essential plan functions. These functions can include managing account contributions and withdrawals, designing plan documents and benefit statements, handling payroll, and holding plan assets in a bank. Some service providers, however, may also sell or use PII and other information to market financial products and services such as loans, annuities, life insurance, and investment advice, according to our review of 31 selected service provider privacy disclosures. Of the disclosures that we reviewed, 29 of 31 did not limit the service provider's ability to share participant data for marketing because they either explicitly allowed it (14) or did not specify whether they would share participant data for this purpose (15). More than half of the selected disclosures (17 of 31) did not limit the service provider's ability to sell participant data (see fig. 2).

Figure 2: Selected 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 Participant Data Sharing Provision

"We may share your personal information with others with your consent, by agreement, or as permitted or required by law. We may share your personal information without your consent if permitted or required by law. For example, we may share your information with businesses hired to carry out services for us. We may also share it with our affiliated or unaffiliated business partners through joint marketing agreements. In those situations, we share your information to jointly offer you products and services or have others offer you products and services we endorse or sponsor. Before sharing your information with any affiliate or joint marketing partner for their own marketing purposes, however, we will first notify you and give you an opportunity to opt out."

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

Plan participants can opt out of having their information shared in some cases, according to our review of selected privacy disclosures. Some disclosures—12 of 31—stated that participants could opt out of having their data shared for marketing. However, opt-out provisions sometimes varied in what they covered, or were not provided at all. For example, one privacy disclosure noted that the service provider may share participant information, when permitted by law, with their affiliated or unaffiliated business partners through joint marketing agreements to offer products and services, or to have others offer products and services that the service provider endorsed or sponsored. Participants are not provided an option to opt out. The disclosure further notes, however, that participants may opt out from affiliates or joint marketing partners using their personal information for their own marketing purposes (e.g., for products or services that are not endorsed or sponsored by the service provider) (see sidebar). Another disclosure stated that the law in most states allowed them to share personal information with their affiliates and participants could not opt out (see sidebar).

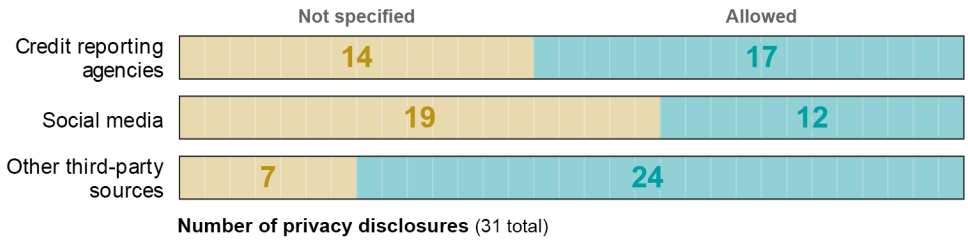
Selected Participant Data Sharing Provision

"In most states, the law allows us to share your information with our affiliates. You may not opt out of these disclosures. We will only share your information as permitted by law."

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

Service providers may independently collect information about participants from sources other than the plan sponsor, including from credit reporting agencies, social media, and other third-party sources, according to our review of selected service provider privacy disclosures. In total, 28 of the 31 selected disclosures stated that the service provider would independently collect data from at least one source other than the plan sponsor. For instance, 24 of 31 disclosures stated that service providers may collect data from other third-party sources, which could include insurance companies, financial advisors, or healthcare providers, according to our review of selected privacy disclosures (see fig. 3).

Figure 3: Selected Retirement Plan Service Provider Policies for Participant Data Collection from Sources Other Than the Plan Sponsor



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

Note: Other third-party sources could include insurance companies, financial advisors, or healthcare providers, according to GAO's review of selected service provider privacy disclosures.

Service provider disclosures reported collecting these data primarily for marketing (15 of 31) and research (13 of 31). For instance, one service provider's disclosure noted that it collected participant information to provide retirement and other financial services and investment products. The information collected could include a participant's investment objectives and experience, financial circumstances, and investment transactions and holdings, according to the disclosure. Another disclosure noted that the service provider collected participant data to test, develop, and improve its products and services or to conduct business analysis and market research.

Plan sponsors can contractually limit service providers from collecting certain types of information or using participant data for marketing. For instance, a plan sponsor we interviewed said that the sponsor included standard language in all contracts with service providers, stating that the provider cannot share participant PII unless explicitly permitted by the plan sponsor. However, research from the Society of Professional Asset Managers and Recordkeepers (SPARK) Institute found that participant data privacy was of greater concern to the larger plan sponsors than the small or mid-sized sponsors that participated in the study.[33] Two of the five record keepers that we interviewed agreed that larger retirement plan sponsors tended to focus more on participant data privacy than smaller plan sponsors. For example, one of the record keepers said that smaller plan sponsors typically lacked the detailed privacy addendums and contractual language that larger plan sponsors might include in their contracts with service providers. Another of the record keepers noted that most plan sponsors did not generally limit the service provider's ability to use participant information to market targeted products or services. Of the six plan sponsor privacy disclosures that we reviewed, two mentioned any collection or use limitations placed on third-party contractors with respect to employee data.

[33]SPARK Institute, *SPARK Study: Understanding Data Privacy Sensitivities Across the Defined Contribution Industry* (Simsbury, CT: Apr. 2023). This industry sponsored study was conducted by the SPARK Institute in collaboration with the Defined Contribution Institutional Investment Association's (DCIIA) Retirement Research Center. As part of the study, DCIIA interviewed or held focus groups with 14 plan sponsors from May to October 2022, which included a mix of small, medium, and large plans. Additionally, an online survey was deployed to DCIIA Plan Sponsor Institute members, with 83 plan sponsors responding. The results of the study are not generalizable.

Plan Service Providers' Use of Data May Potentially Benefit Participants but Also Increase Privacy Risks

Use and dissemination of participant data by plan sponsors and service providers beyond what is necessary to administer the plan can potentially benefit participants. For instance, record keepers said they offered financial wellness programs, which are intended to provide participants with a holistic view of their financial health including retirement savings, emergency savings, spending, and debt. Using personal participant data to match participants to appropriate financial products or services could benefit participants, particularly those that might find managing their retirement savings to be complex or overwhelming. A record keeper said that the company used participant data to deliver targeted training on various topics including investing, budgeting, and preparing for retirement. The record keeper also said that it offered participants opportunities to meet with financial advisors to discuss their individual financial goals and different products or services that may help them meet those goals. Sharing participant data with researchers may also be useful for learning more about participant behavior or plan performance, with potential insights for how to help participants save more for retirement.

Sharing participant data for purposes beyond plan administration, however, may increase risk of identity theft, fraudulent activity, or unwanted marketing. While not limited to retirement plan participants, the Department of Justice estimated that about 24 million U.S. residents 16 years or older had been victims of identity theft during the prior 12 months, with financials losses totaling $16.4 billion in 2021, the most recent data available.[34] In addition, we have reported previously that as technologies change, consumers might not always know what data businesses are collecting about them, or how those data are used and shared.[35] Advanced technologies help businesses gather increasing amounts of personal data, track online behavior, and monitor consumers' locations and activities, intensifying concerns about the privacy and accuracy of consumer data. In addition, information resellers—sometimes called data brokers—collect a vast amount of information about consumers and then aggregate and sell it.[36] Resellers can include companies like credit reporting and marketing agencies that obtain participant PII and financial data from plan service providers, according to our review of selected privacy disclosures. CFPB reported in December

[34]Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2021* (Washington, D.C.: Oct. 2023).

[35]GAO, *Consumer Data: Increasing Use Poses Risks to Privacy*, GAO-22-106096 (Washington, D.C.: Sept. 2022).

[36]GAO-13-663.

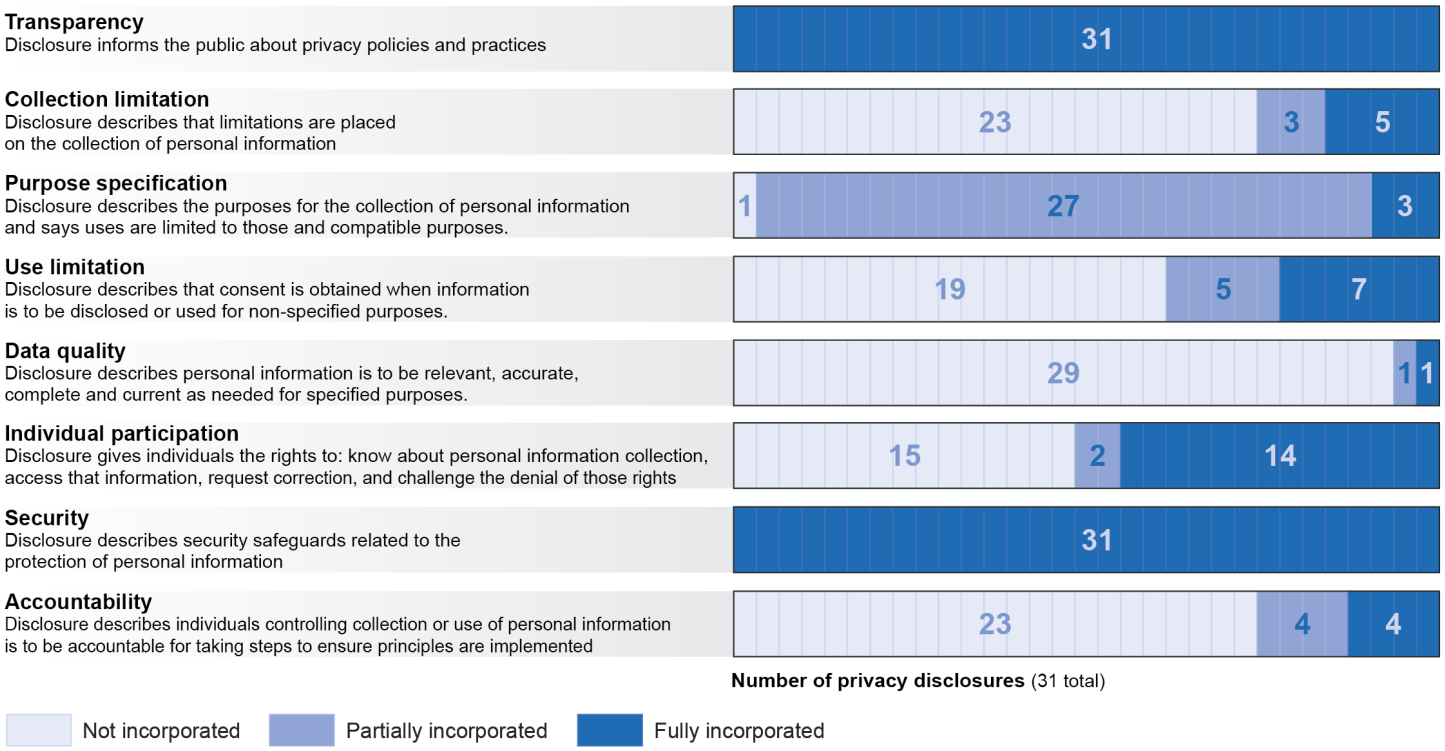
2024 that by selling personal information about consumers without their knowledge or consent, data brokers could profit by enabling scamming, stalking, and spying on U.S. consumers.[37]

Selected Service Providers Inform Consumers of Privacy Policies, but Disclosures Do Not Fully Incorporate Leading Privacy Practices

Selected service provider privacy disclosures that we reviewed did not consistently incorporate leading privacy practices, as reflected in the Fair Information Practice Principles (FIPP). The FIPPs provide a framework for responsible data handling, emphasizing key privacy protection principles such as transparency in data practices, purpose specification to define intended uses, and restrictions to prevent unauthorized use of personal data. All 31 selected service providers had publicly available privacy disclosures that described their policies for using personal information and described how personal information would be protected, which is consistent with two FIPPs: transparency and security. However, many of the disclosures varied in how they incorporated the principles of collection limitation, purpose specification, use limitation, data quality, individual participation, and accountability. Figure 4 shows the number of disclosures that fully, partially, or did not incorporate these principles.

[37]CFPB published a proposed rule in December 2024 that aimed to limit data brokers from selling sensitive personal and financial information about U.S. consumers. In May 2025, CFPB withdrew the proposed rule.

Figure 4: Incorporation of Fair Information Practice Principles (FIPP) into 31 Selected Retirement Plan Service Provider Privacy Disclosures



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

As shown in figure 4, the service provider disclosures generally addressed the principles of transparency and security, but many of the disclosures did not fully align with other FIPPs:

Transparency. All 31 selected service providers had publicly available privacy disclosures describing their policies related to their use of personal information, although these varied in the details provided. For example, one disclosure explains how the organization may collect, use, and disclose personal information, including the reasons why. Additionally, it describes the categories of personal information collected, how it is used, with whom the organization may share it, the business purposes for doing so, and the rights individuals have. In contrast, other disclosures offer only a high-level statement about collecting personal information for general business purposes without specifying data categories, sharing practices, or individual rights.

Collection limitation. Five of the disclosures that we reviewed described that personal information collection would be limited to what was needed for stated business purposes, but most (26 of 31) did not clearly describe collection limitations. For example, one disclosure states that the service provider will not collect certain types of information about participants (e.g., medical information) but does not specify any other limitations, such as collecting only the minimum necessary data.

Purpose specification. Three service providers included an explanation of the reasons for collecting personal information and the restrictions on its use. For example, one disclosure states that the processing of personal information will be limited to business information related to the individual, among others. However, most (28 of 31) service provider disclosures lacked clarity regarding either the specific purposes for which information was collected, or whether its use was limited to those purposes. For example, one disclosure defines collection purposes such as managing accounts, processing transactions, and offering products and services, but it does not specify that uses will be restricted to those purposes.

Use limitation. Some (seven of 31) service provider disclosures prohibited the use of personal data for unrelated purposes without additional consumer consent. For example, one disclosure states that consent from the individual may be required when a new or different business purpose is identified for processing personal data. Other disclosures (five of 31) partially addressed use limitations. For example, one disclosure states the service provider will not disclose a person's voiceprint unless required by law or with an individual's consent but did not identify such limitations for other types of data.

However, most of the service provider disclosures we reviewed (19 of 31) did not clearly state that additional consent would be sought before sharing or otherwise using personal information beyond originally specified purposes. For example, one disclosure states that additional disclosures will be provided in cases where data collection is materially different than what is described in the policy. However, the disclosure does not mention a process for obtaining additional consent from participants to use their data for purposes beyond those initially stated. Other disclosures were silent on use limitations, leaving it unclear whether further consent would be sought for expanded uses.

Data quality. One disclosure describes the provider's commitment to setting appropriate standards for data quality. For example, the disclosure

states that the provider will take steps to ensure that personal data is accurate and current, as needed for processing. Another disclosure partially describes the provider's data quality practices. For example, the disclosure acknowledges that individuals have the rights to request that inaccurate information is (1) corrected and (2) not processed. However, 29 of the service provider disclosures reviewed did not provide specific details about their data quality practices, leaving it unclear what steps the providers take to ensure the relevance and accuracy of the data collected.

Individual participation. Many disclosures (14 of 31) indicated that individuals may access and update their personal information. For example, one disclosure allows individuals to request access to their personal information. Additionally, the disclosure indicates that individuals can request corrections or updates to their personal data using the provided contact methods to address inaccuracies. The remaining 17 disclosures either limited their discussion to certain states that have privacy laws or were silent on the matter. For example, some disclosures reference additional rights based on the privacy laws of the individual's state of residence, while others provide no guidance on how individuals can exercise their rights to access or correct their personal data.

Security. All 31 disclosures described various measures to protect personal information. For example, one disclosure describes staff training on privacy risks, technical safeguards like firewalls, encryption, antivirus software, and physical security controls. It also states that the organization ensures system resilience, restricts access, and conducts external audits and vendor due diligence. The disclosure also mentions real-time data leakage monitoring and security incident management.

Accountability. Four out of 31 disclosures specified how the organization took responsibility for data protection practices. For example, one disclosure outlines measures to protect personal data and specifies how the organization takes responsibility for data protection practices, to include having oversight from an audit committee and leadership from a global chief privacy officer to ensure robust privacy governance across the organization's operations. Four disclosures partially addressed accountability. For example, one disclosure states that the company ensures compliance with data protection laws but does not provide additional details on its accountability measures. The remaining 23 disclosures were silent on their accountability measures.

Incorporating leading data privacy practices can reduce privacy risks for retirement plan participants. For example, explicitly limiting how data can be used beyond clearly specified purposes could reduce a participant's risk of identity theft and other unwanted uses of personal information. Further, obtaining consent from participants before sharing their data could help to ensure that participants understand which third parties have access to their data and how those entities may use their information. The FIPPs are not legal requirements, but such frameworks could assist service providers in ensuring transparent privacy policies and proper safeguarding of participant information.

Federal Agencies and States Have Taken Steps to Oversee Data Privacy, but DOL Has Not Provided Sufficient Guidance on Retirement Plans' Use of Participant Data

DOL and Federal Agencies that Enforce Consumer Privacy Laws Have Not Taken Actions Against Retirement Plans for Sharing Participant Data

DOL and officials from federal agencies that enforce consumer data privacy laws said that they have not taken actions against retirement plans for sharing participant data, citing various reasons. DOL officials said that they have not taken enforcement actions against retirement plan sponsors or service providers specifically related to the use or sharing of participant data. They said this is in part because ERISA does not discuss data privacy explicitly. DOL officials said that ERISA assumes that plan sponsors will share certain information with service providers for plan administration purposes. However, these officials also said that ERISA requires plan fiduciaries to behave prudently and loyally with respect to their management of ERISA plans, which means taking reasonable steps to safeguard participant data.

SEC, FTC, and CFPB have some authority to enforce consumer data privacy laws, but officials from these agencies said that their authority depends on certain facts and circumstances.

- FTC officials stated that the relevant federal laws do not provide clear guidelines with respect to allowed or prohibited sharing or use of personal information outside of the specific sector or population for which those laws apply. Further, they said that the laws they enforce do not apply specifically to retirement plans and may not be applicable to all the parties involved in administering DC plans. For example, GLBA, which focuses on financial institutions, may not apply to plan sponsors or certain retirement plan service providers that mostly handle administrative duties for the plan sponsor. FTC exercises privacy oversight through its enforcement of Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce.

- SEC officials stated that while the agency has limited authority for data privacy for retirement plan sponsors, it does have such authority for certain plan service providers, such as registered investment advisors and broker dealers. Its authority falls under Regulation S-P, which is a set of privacy rules adopted pursuant to GLBA and the Fair and Accurate Credit Transactions Act of 2003 that govern the treatment of nonpublic personal information about consumers by certain financial institutions, according to SEC.[38]

- CFPB officials stated that retirement plans are excluded from the agency's jurisdiction because federal law specifies that such plans are not consumer financial products or services. In addition, officials noted that the federal law states that CFPB may not exercise any rulemaking or enforcement authority with respect to

[38]A broker is any person engaged in the business of buying or selling securities for the account of others. A dealer is any person engaged in the business of buying or selling securities, but for their own account, according to SEC. Nearly all broker-dealers doing public business in the United States must be members of FINRA. FINRA is responsible under federal law for supervising member firms and issues rules and guidance for complying with federal securities laws and regulations, including those pertaining to the privacy and security of customer data.

products or services that relate to any specified employee benefit or compensation plan or arrangement.[39]

Retirement plan participants have filed at least 11 lawsuits from 2009 through 2024 in federal courts that allege that plan sponsors breached their fiduciary duty under ERISA by failing to prevent contracted service providers from using participant data for their own purposes, and subjected participants to unwanted marketing. As of December 2024, seven of these cases had been settled. While the settlement agreements included no finding of liability on behalf of the plan sponsors, five included agreements by the plan sponsor to add contractual language preventing service providers from using participant data for marketing.

Data Privacy Laws in Certain States Provide Consumers the Right to Opt-Out of Data Sharing, but State Officials Said These Laws May Not Apply to Retirement Plans

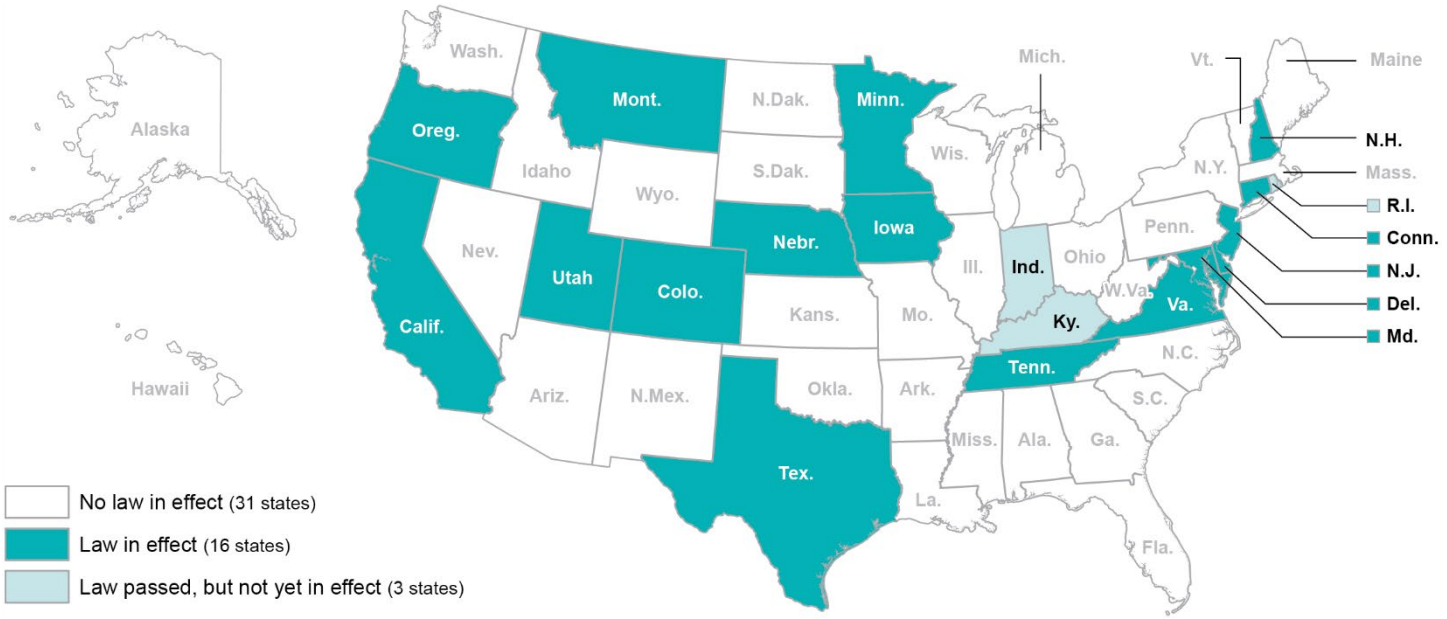
As of November 24, 2025, 19 states have enacted comprehensive data privacy laws that have already taken effect or that will do so in 2026 (fig. 5).[40] In contrast to related federal laws, these state laws generally apply with certain exceptions across a broad range of entities.[41] In 2018, California was the first state to enact such legislation, which took effect in January 2020, followed by legislation enacted in Virginia and Colorado in 2021 and which took effect in January 2023 and July 2023, respectively.

[39]See 12 U.S.C. § 5517(g).

[40]To understand comprehensive data privacy laws that have been enacted in various states, we reviewed research from IAPP and interviewed IAPP officials. IAPP's research on state privacy laws tracks proposed and enacted privacy bills from across the U.S. that are comprehensive rather than narrow in scope. According to IAPP, a bill is narrow in scope if (1) it applies only to a specific set of data types, like financial or health data, or data subjects, like children, (2) its applicability includes only a single industry, like the automotive industry, or if its thresholds apply, in practice, to only a handful of companies, or (3) it is targeted at providing only one or two consumer data rights, such as deletion or correction. To complement our review of existing research, we also interviewed or obtained information from officials in three selected states—California, Colorado, and Virginia—to discuss how their state privacy laws may apply to retirement plans. For additional information on our review of state privacy laws, see app. I.

[41]State privacy legislation may exempt certain types of entities. For instance, California's privacy legislation does not generally apply to nonprofit organizations or government agencies.

Figure 5: U.S. State Data Privacy Laws, as of November 24, 2025



Source: GAO review of International Association of Privacy Professionals (IAPP) State Privacy Legislation Tracker. | GAO-26-107271

All or almost all of the comprehensive state privacy laws provide consumers the right to opt out of having certain personal information sold (19 of 19) or shared (18 of 19). Under these states' laws, if consumers do not exercise these rights, business are free to sell or share personal information about consumers. Most of the state privacy laws (17 of 19) also allow consumers to review any personal information companies may hold about them and to request that errors be corrected, if applicable. Under California law, for instance, certain businesses must provide at least two methods, such as a designated telephone number or web-based option, that consumers can use to request, review, and correct personal information held about them or to exercise their right to opt out of having their personal information sold or shared for marketing.

Officials that we interviewed or obtained information from in selected states—California, Colorado, and Virginia—stated that it was uncertain if the privacy laws in their states applied to retirement plan sponsors or service providers given potential ERISA pre-emption. Specifically, ERISA includes a provision stating that ERISA generally supersedes state laws that "relate to" any employee benefit plan covered under ERISA. In addition, officials stated that the laws in their states include certain exemptions for financial institutions that are subject to GLBA. These

officials also stated that they had not taken any enforcement actions to date against plan sponsors or service providers for noncompliance with state privacy laws.

DOL Has Not Provided Sufficient Guidance on Retirement Plans' Use of Participant Data

DOL issued cybersecurity guidance for retirement plan sponsors and services providers in April 2021, following GAO and ERISA Advisory Council reports that raised concerns about the security of retirement plan assets and data.[42] DOL's guidance discusses data privacy as a component of plan cybersecurity. For instance, the guidance states that plan sponsors should

- ensure service provider contracts clearly address the providers' obligation to keep private information private,
- prevent the use or disclosure of confidential information without written permission, and
- meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse.

The guidance further states that service providers should have a formal and well-documented cybersecurity program, which includes effective policies and procedures governing data privacy, among other things.

However, DOL's guidance does not provide examples of acceptable uses of participant data, define what information it considers to be private, or describe the types of situations in which service providers should obtain permission to use or disclose information about participants. Given the many ways that service providers use and share participant data to administer a retirement plan, it may be difficult for service providers to

[42]DOL issued three forms of cybersecurity guidance: (1) Tips for Hiring a Service Provider with Strong Cybersecurity Practices, (2) Cybersecurity Program Best Practices, and (3) Online Security Tips. DOL updated this guidance in September 2024 to clarify that it applies to all plans covered by ERISA, including health plans and all employee retirement benefit plans. The Advisory Council on Employee Welfare and Pension Benefit Plans, usually referred to as the ERISA Advisory Council, was established under Section 512 of ERISA to advise the Secretary of Labor on matters related to welfare and pension benefit plans. The council consists of 15 members appointed by the Secretary of Labor, which includes representatives from employee organizations, employers, the general public, and the fields of insurance, corporate trust, actuarial counseling, investment counseling, investment management, and accounting. Advisory Council on Employee Welfare and Pension Benefit Plans, *Cybersecurity Considerations for Benefit Plans* (Washington, D.C.: Nov. 2016) and Advisory Council on Employee Welfare and Pension Benefit Plans, *Privacy and Security Issues Affecting Employee Benefit Plans* (Washington, D.C.: Nov. 2011), and GAO-21-25.

determine when they should obtain consent. Finally, the guidance also does not refer to leading privacy practices as benchmarks for plan sponsors or service providers managing of participant data.

Within DOL, EBSA's mission is to ensure the security of the retirement, health, and other job-based benefits of America's workers and their families. One way the agency accomplishes its mission is by assisting and educating workers, plan sponsors, fiduciaries, and service providers on their responsibilities. Further, federal internal control standards state that agencies should externally communicate the necessary quality information to achieve the agency's objectives.[43]

In April 2023, the SPARK Institute found that plan sponsors and record keepers that participated in the study wanted DOL to create industry data privacy standards, given the lack of comprehensive national data privacy legislation, differing state requirements, and concerns about lawsuits.[44] Plan sponsors and record keepers that participated in the study also expressed concerns about ensuring adequate flexibility and not adding additional complexity or administrative cost. Of the record keepers that we interviewed, all five said that additional DOL guidance on participant data privacy would be helpful. An ERISA attorney stated that DOL guidance should encourage plan sponsors and service providers to clearly and transparently disclose their privacy policies, allow participants to make informed decisions about how their personal information may be used or shared, and be feasible to implement. Another ERISA attorney suggested that DOL's guidance should be tailored to different plan sizes and types since larger plans may have more capabilities than smaller plans.

DOL officials said that issuing additional guidance on participant data privacy could be beneficial but noted that several factors must be considered. For instance, they said that such guidance would need to

[43]GAO-14-704G.

[44]SPARK Institute, *SPARK Study*. This industry sponsored study was conducted by the SPARK Institute in collaboration with the Defined Contribution Institutional Investment Association's (DCIIA) Retirement Research Center. As part of the study, DCIIA interviewed or held focus groups with 14 plan sponsors from May to October 2022, which included a mix of small, medium, and large plans. Additionally, an online survey was deployed to DCIIA Plan Sponsor Institute members, with 83 plan sponsors responding. In addition, DCIIA interviewed six large record keepers. The results of the study are nongeneralizable.

balance the legitimate need for plan sponsors and service providers to use and share participant data to administer a retirement plan. In addition, DOL officials said that such guidance must provide some flexibility to ensure it does not hinder data sharing that could benefit participants. The FIPPs, or other privacy best practices, could provide the basis of guidance for responsible plan data collection, use, and sharing that protects participant privacy, but does not excessively burden plan sponsors and service providers, and allows participants to choose products and services that may help them save for retirement and manage their accounts.

DOL officials said that they had not issued additional guidance on participant data privacy because the agency believes that ERISA's duties of prudence and loyalty, as well as ERISA's prohibited transaction requirements, should sufficiently deter plan sponsors and service providers from unauthorized uses of participant data. Nevertheless, most of the selected privacy disclosures that we reviewed did not limit the service providers' ability to share or sell participant data for marketing. 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.

Conclusions

Plan sponsors and service providers often decide how to collect and use participant data based on their own business interests. DOL issued cybersecurity guidance to retirement plan sponsors and service providers in April 2021 that acknowledged data privacy as a component of cybersecurity and included some general data privacy expectations. However, DOL's guidance did not include what participant information should be considered private and the types of situations in which service providers should obtain written permission to use or disclose such information. Developing and issuing such guidance could benefit participants by better protecting their personal information and shielding them from unwanted marketing, while also allowing them to exert more choice about how their data may be used and shared. Direction around data collection and use could also benefit service providers, which would have clearer expectations about what uses of participant data are allowed and when they should seek permission before using or sharing participant data. The FIPPs, or other privacy best practices, could provide the basis for such guidance. By incorporating such best practices into guidance, DOL would help ensure that providers have the information they need to

make responsible decisions about how they are collecting and using participants' data.

Recommendations for Executive Action

The Secretary of Labor should provide additional guidance about participant data privacy for retirement plan sponsors and service providers. In particular, the Secretary should clarify what participant information should be considered private and the circumstances in which service providers should obtain written permission before using or sharing this information. Such guidance could also identify best practices including for providing individual participants with choice, to the extent practicable, about how their personal information may be used, sold, or shared. (Recommendation 1)

Agency Comments and Our Evaluation

We provided a draft of this report to DOL for review and comment. DOL provided written comments, which are reproduced in appendix II. We also provided pertinent excerpts from the draft to CFPB, SEC, and FTC for review and comment. We received technical comments from CFPB, SEC, FTC, and DOL, which we have incorporated into the report as appropriate.

In its written comments, DOL neither agreed nor disagreed with our recommendation, noting that the Department will carefully consider, as resources permit, whether supplemental guidance aligned with the recommendation could or should be issued. DOL noted that its 2021 cybersecurity guidance states that a prudent fiduciary should make sure that contracts contain "clear provisions on the use and sharing of information" and that the contract "should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse." DOL's guidance, however, describes neither what information should be considered private, nor what are acceptable uses of such information. Given the many ways that service providers may use and share participant data, including for marketing, additional guidance would help ensure service providers have sufficient clarity on how to appropriately use and share participant data.

This report cites various reasons why we believe more specific guidance is warranted. According to our review of selected service provider privacy disclosures, most service providers did not limit their ability to share or sell participant data for marketing purposes, and in some cases prevented participants from opting out of sharing of their personal data.

Many of these disclosures reflected policies that did not fully incorporate leading privacy practices, such as collection or use limitations. This report acknowledges that some participants may potentially benefit from limited marketing based on their shared personal data, but also that such sharing may increase privacy risks for participants. Additionally, industry sponsored research found that plan sponsors and record keepers wanted DOL to create industry data privacy standards, given the lack of comprehensive national data privacy legislation, differing state requirements, and concerns about lawsuits. Implementing the recommendation could benefit participants by better protecting their personal information as well as plan sponsors and service providers by clarifying acceptable uses of participant information.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Labor and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff should have any questions about this report, please contact Tranchau (Kris) Nguyen at nguyentt@gao.gov or Marisol Cruz Cain at cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

//SIGNED//

Tranchau (Kris) Nguyen
Director, Education, Workforce, and Income Security Issues

//SIGNED//

Marisol Cruz Cain
Director, Information Technology and Cybersecurity Issues

Appendix I: Objectives, Scope, and Methodology

This report examines (1) how retirement plan service providers and sponsors use and share participant data and the potential benefits and risks of current data sharing practices, (2) how selected retirement plan service provider policies incorporate leading practices for data privacy, and (3) how federal agencies and selected states oversee consumer data privacy as it applies to retirement plans.

To address the first objective, we reviewed a nongeneralizable sample of publicly available privacy disclosures. Specifically, we reviewed publicly available privacy disclosures from 21 record keepers and 10 asset managers for a total of 31.[1] We reviewed each of these disclosures to identify the types of data being collected, the stated sources of this information (e.g., credit reporting agencies, social media, or other third-party sources), and the extent to which record keepers and asset managers stated that they used, shared, or sold participant data for targeted marketing.

To identify record keepers, we consulted with representatives from the Society of Professional Asset Managers and Recordkeepers (SPARK) Institute and used their membership list as a basis for our selection. The SPARK Institute's publicly available membership list included 551 members as of August 2024. However, since many entities had multiple members, we removed duplicates to identify the unique number of entities represented—which resulted in 109, according to our review. We then reviewed each entity's website to identify if it operated independently rather than as a subsidiary of another listed member, which reduced the list to 98. We further reviewed these websites to confirm that the 98 selected entities provided record keeping services (as opposed to other ancillary services such as software support services) and had privacy disclosures publicly available, which reduced the list to 34. We then contacted each of these record keepers to confirm that the disclosures that we had identified applied specifically to their record keeping services, of which 21 responded and were included in our review. We excluded the remaining 13 record keepers that did not respond to our attempts to verify their privacy disclosures.

To identify asset managers, we used data from *Pensions and Investments*, which is a retirement industry publication that provides

[1]The findings from our review of selected privacy disclosures are not generalizable and cannot be used to make inferences about the entire population of record keepers or asset managers.

institutional investment data and analysis on service providers.[2] Specifically, we selected the 10 largest asset managers by the amount of institutional assets invested as of December 31, 2022, the most recent data available. For these asset managers, we reviewed privacy disclosures that were applicable to their investment services specifically or those marked as "global" or United States-specific, as applicable.

We also reviewed publicly available privacy disclosures from six selected retirement plan sponsors.[3] We reviewed these disclosures to identify what, if any, limitations these sponsors placed on service providers, like record keepers and asset managers, about how they could use, share, or sell participant data. To identify plan sponsors, we used data from *Pensions and Investments*.[4] We selected the 10 largest defined contribution retirement plan sponsors by the amount of retirement assets invested as of September 30, 2022, the most recent data available. However, only six of the 10 selected plan sponsors had publicly available privacy disclosures available that were specific to employees.[5] Therefore, we excluded the remaining four plan sponsors from review.

To understand the benefits and risks of current data sharing practices, we interviewed or obtained information from a total of 26 stakeholders. These included retirement industry associations such as the American Retirement Association, SPARK Institute, and the Employee Retirement

[2]"The Largest Money Managers 2023," *Pensions and Investments*, June 12, 2023.

[3]The findings from our review of selected privacy disclosures are not generalizable and cannot be used to make inferences about the entire population of plan sponsors.

[4]"Largest U.S. Retirement Plans 2023," *Pensions and Investments*, Feb. 13, 2023.

[5]For plan sponsors, our review focused on employee specific privacy disclosures instead of customer specific disclosures aimed at those who may do business with the company or purchase its products or services.

Income Security Act (ERISA) Industry Committee.[6] We also interviewed or obtained information from researchers, plan sponsors, record keepers, attorneys specializing in ERISA or data privacy, retirement plan consultants, and groups that advocate on behalf of retired people, including the Pension Rights Center and AARP. During these interviews, we discussed how plan sponsors and service providers might use and share data about plan participants and the purposes for doing so. We also discussed what, if any, safeguards or limitations plan sponsors or service providers might take to protect participant privacy. Further, we interviewed officials from data privacy groups including the World Privacy Forum, Electronic Frontier Foundation, and IAPP to discuss consumer data privacy more generally and the potential benefits and risks of sharing personally identifiable information (PII) and financial information about consumers.[7] Lastly, we met with officials from the Department of Labor (DOL), which oversees retirement plans and benefits, as well as other federal agencies involved in overseeing consumer data privacy laws, including the Consumer Financial Protection Bureau (CFPB), Securities and Exchange Commission (SEC), and Federal Trade Commission (FTC).

To address the second objective, we reviewed the selected record keeper and asset manager privacy disclosures as described above using the Fair Information Practice Principles (FIPP). With some variation, the FIPPs have been widely used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United

[6]To identify relevant retirement stakeholders, we began by interviewing individuals, groups, and organizations that participated in a prior related GAO review. See GAO, *Defined Contribution Plans, Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans,* GAO-21-25 (Washington, D.C.: Feb. 2021). During these interviews, we asked stakeholders to recommend other relevant individuals, groups, or organizations that we should contact to discuss how retirement plan sponsors and service providers use and share data about plan participants, as well as those that focus on consumer data privacy more generally. The 26 stakeholders interviewed specifically included four retirement industry associations, five record keepers, two plan sponsors, two retirement plan consultant groups, three attorneys with ERISA or data privacy specialization, two retirement advocacy groups, four data privacy researchers or associations, and four federal agencies. The interviews conducted are not generalizable and cannot be used to make inferences beyond the individuals, groups, or organizations that participated in our review.

[7]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number; and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

States.[8] While the FIPPs are not precise legal requirements, they provide a framework for balancing the need for privacy with other interests. Table 3 describes the eight individual principles that constitute the FIPPs.

Table 3: Fair Information Practice Principles (FIPP)

Principle	Description
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Co-operation and Development. | GAO-26-107271

To conduct our review, we reviewed the content of each privacy disclosure to identify key elements related to consumer privacy protection. These included:

- Types of personal information collected,
- Purposes for data collection,
- Data sharing practices, including disclosures to third parties,

[8]The FIPPs served as the basis for the Privacy Act of 1974, which governs the collection, maintenance, use, and dissemination of personal information by federal agencies.

- Consumer rights regarding their personal information, and
- Security measures in place to protect data.

We then determined the extent to which the identified practices were in alignment with the relevant FIPPs. Specifically, we assessed the extent to which the selected disclosures fully incorporated, partially incorporated, or did not incorporate each of the FIPPs. We determined that the disclosures fully incorporated the FIPP if the practices described aligned with all elements of the principle, partially incorporated the FIPP if the practices aligned with some, but not all elements of the principle, and did not incorporate the FIPP if the practices did not align with any elements of the practices. The assessment was used to support our analysis of the disclosures' content and structure; however, it was not intended to evaluate compliance with the FIPPs.

To address the third objective, we reviewed relevant federal laws and regulation including ERISA and the Gramm-Leach-Bliley Act, among others. We also interviewed federal officials from DOL, CFPB, SEC, and FTC to discuss their oversight and enforcement of relevant federal law and regulations with respect to retirement plan sponsors and service providers. We also reviewed DOL's cybersecurity guidance issued in 2021 for retirement plan sponsors and service providers to understand the extent to which data privacy was included as a component of cybersecurity.[9] Further, we assessed DOL's cybersecurity guidance in relation to relevant federal internal control standards for information and communication.[10]

We also identified and reviewed relevant cases filed in federal courts to provide examples of complaints participants have alleged about sharing of their personal information by plan sponsors or service providers. Specifically, we performed a key word search using a legal database to identify cases that specifically included an allegation that a plan sponsor or service provider had used plan data without consent for targeted marketing. While not generalizable, reviewing these cases also allowed us to provide examples of actions plan sponsors have taken to address

[9]DOL updated its cybersecurity guidance in September 2024 to clarify that it applies to all plans covered by ERISA, including health plans and all employee retirement benefit plans.

[10]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

such allegations as part of settlement agreements reached between parties.

To understand comprehensive data privacy laws that have been enacted in various states, we reviewed research from IAPP and interviewed IAPP officials.[11] IAPP is a not-for-profit organization and certification body that publishes research on state level privacy legislation. It also assists companies and institutions in managing and protecting data, provides a forum for privacy professionals to share best practices, and track trends, among other things. IAPP's research on state privacy laws tracks proposed and enacted privacy bills from across the U.S. that are comprehensive rather than narrow in scope. According to IAPP, a bill is narrow in scope if (1) it applies only to a specific set of data types, like financial or health data, or data subjects, like children; (2) its applicability includes only a single industry, like the automotive industry, or if its thresholds apply, in practice, to only a handful of companies; or (3) it is targeted at providing only one or two consumer data rights, such as deletion or correction.[12]

To complement our review of existing research about state privacy laws, we also interviewed or obtained information from officials in three selected states—California, Colorado, and Virginia—to discuss how their state privacy laws might apply to retirement plans.[13] We selected these states because their data privacy laws have been in effect the longest. In 2018, California was the first state to enact such legislation, which took effect in January 2020, followed by legislation enacted in Virginia and Colorado in 2021 and which took effect in January 2023 and July 2023, respectively.

We conducted this performance audit from January 2024 to February 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

[11]IAPP, *US State Comprehensive Privacy Laws Report, 2023 Legislative Session* (Portsmouth, NH: January 2024) and IAPP, *US State Privacy Legislation Tracker* (Portsmouth, NH: Nov. 24, 2025).

[12]IAPP, *Defining 'Comprehensive': Florida, Washington and the Scope of State Tracking* (Portsmouth, NH: Feb. 22, 2024).

[13]We interviewed or obtained information from officials from the California Privacy Protection Agency and from State Offices of Attorney General in Colorado and Virginia.

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Labor

U.S. Department of Labor

Assistant Secretary for
Employee Benefits Security Administration
Washington, D.C. 20210

February 4, 2026

Tranchau (Kris) Nguyen
Director, Education, Workforce, and Income Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Nguyen:

Thank you for the opportunity to review the Government Accountability Office (GAO) report titled "Defined Contribution Retirement Plans: DOL Guidance Could Help Mitigate Privacy Risks for Participants" (GAO-26-107271). Below, we provide the Department of Labor's (Department) response to the report's recommendation.

GAO Recommendation

The Secretary of Labor should provide additional guidance about participant data privacy for retirement plan sponsors and service providers. In particular, the Secretary should clarify what participant information should be considered private and the circumstances in which service providers should obtain written permission before using or sharing this information. Such guidance could also identify best practices for providing individual participants with choice, to the extent practicable, about how their personal information may be used, sold, or shared.

Department of Labor Response

The Department fully supports the goal of appropriately protecting the personal information of participants and beneficiaries of plans covered by the Employee Retirement Income Security Act of 1974 (ERISA). However, the Department neither agrees nor disagrees with the report's recommendation.

As reflected throughout the report, the Department's 2021 fiduciary guidance on cybersecurity references data privacy as a component of cybersecurity. This guidance, in relevant part, clearly and unequivocally states that when a fiduciary contracts with a service provider, a prudent fiduciary makes sure that the contract contains clear provisions on the use and sharing of information. The guidance also states that the contract "should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse."

The Department believes that the general principles articulated in the 2021 guidance make clear that ERISA's fiduciary provisions obligate fiduciaries to, among other things, include data privacy considerations in the contracting process for service providers. However, as resources permit, the Department will carefully consider whether supplemental guidance aligned with the recommendation could or should be issued.

Thank you again for the opportunity to review the draft report and recommendations. Please contact us if you have any questions concerning this response or if we can be of further assistance.

Sincerely,

DANIEL ARONOWITZ

Digitally signed by DANIEL ARONOWITZ
Date: 2026.02.04 17:16:31 -05'00'

Daniel Aronowitz
Assistant Secretary

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Tranchau (Kris) Nguyen at nguyentt@gao.gov

Marisol Cruz Cain at cruzcainm@gao.gov

In addition to the contacts named above, Mark Glickman (Assistant Director), Lee McCracken (Assistant Director), Justin Dunleavy (Analyst in Charge), Sher'rie Bacon, Alexis Hartranft, and Shaunyce Thurman made key contributions to this report. Andrew Bellis, James Bennett, Jillian Clouse, Caitlin Cusati, Swati Deo, Alex Galuten, Rebecca Gertler, Tom Moscovitch, Scott Pettis, and Joy Solmonson also made important contributions.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us