

A Consumer-Centric
Retirement System –

Unlocking Holistic Retirement Planning while Safeguarding Consumer Data

DATE

August 5, 2025

AUTHOR

Lisa M. Gomez,

Former Assistant Secretary of Labor for Employee
Benefits Security, U.S. Department of Labor



Contents

Executive Summary 1

Meeting Consumers Where They Are:
Leveraging Digital Tools for Retirement Planning 2

Consumers Routinely Authorize Digital Tools for
Holistic Planning 3

Custodians and Recordkeepers Also Offer
Consumer-Authorized Tools 3

Consumer-Authorized Technologies Can be
Consistent with Regulatory Requirements 4

Recommendations for a Consumer-Centric
Retirement Planning Ecosystem 5

Disclaimer: The material provided herein is general and is not intended to be legal advice. Nothing in this white paper should be relied upon as legal advice or legally binding. The opinions in this paper are those of its author, and are not intended to represent the opinions of any of the author's former employers, including the U.S. Department of Labor.

1 Executive Summary

People increasingly look to both technology and financial advisors to prepare for retirement. As part of their planning services, financial advisors increasingly use digital tools to get a holistic view of their clients’ finances, including the savings in their 401(k) or other retirement accounts accrued through their working careers. This white paper establishes a foundational knowledge of consumer-authorized technologies that trusted financial advisors use to view and manage their clients’ 401(k) and other retirement accounts, and offers recommendations for plan sponsors, recordkeepers, financial advisors, and regulators in considering these technologies.

This white paper makes the case that, when conducted with appropriate security measures and other safeguards that are prudent and in the interests of the retirement

saver, consumer-authorized data aggregation can be not only consistent with fiduciary responsibilities, but also essential for meaningfully empowering retirement savers. This paper discusses how consumer-authorized data aggregation helps retirement savers prepare for the future, and argues that industry can enable consumer-authorized technologies in ways that enhance both consumer control and cybersecurity, charting the path forward for consumer-centric retirement planning.

Policymakers and the retirement industry should learn about and recognize the benefits of consumer-authorized tools in retirement savings and wealth management, and encourage their safe and secure use in a manner that is in the interest of advancing retirement outcomes for all Americans.

2 Meeting Consumers Where They Are: Leveraging Digital Tools for Retirement Planning

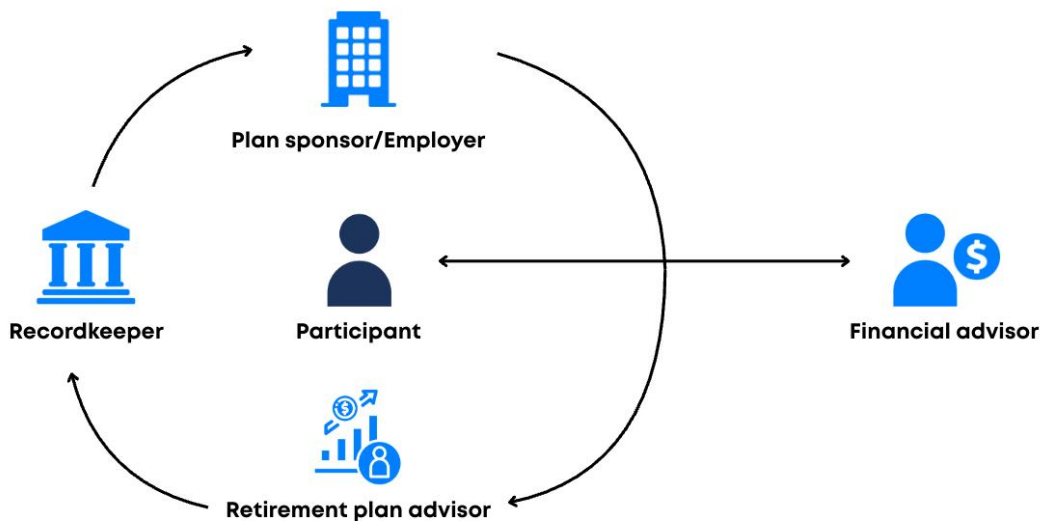
For many people, a 401(k) or other workplace-based retirement account represents a significant portion of their assets. These accounts, however, often exist in a silo, separate from the person's other investments, bank accounts, and liabilities. In today's interconnected world, individuals actively seek holistic solutions for financial planning and retirement preparedness. The proliferation of personal finance apps, investment platforms, and retirement planning tools reflects a growing consumer desire for convenience, accessibility, and a unified approach to financial management.

As detailed in various industry reports, including insights consistent with the findings from a [Visa report](#) on consumer financial tool adoption, individuals are increasingly comfortable and reliant on authorized third-party applications to help them navigate complex financial landscapes. These tools can provide personalized insights, track progress towards goals, and often offer advanced analytical capabilities that a single financial provider's portal or tool might not. In fact, the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) – the regulatory agency I led charged with overseeing all of the private employer-sponsored retirement plans covering America's workers – itself has online [retirement tools](#) and provides access to resources offered by other groups.

For workplace-based retirement plans, the assets of the plan are held in a trust established by the employer or other plan sponsor as required by the Employee Retirement Income Security Act of 1974 (ERISA), 29 U.S.C. Section 1001 et seq. In many cases,

a custodian (often a bank or investment firm) physically holds the plan assets and processes transactions, while a recordkeeper tracks account balances, contributions, and investment elections. The custodian and recordkeeper are usually service providers hired by the plan. The custodian and recordkeeper can be (but are not required to be) the same company, and often are with 401(k) and other retirement plans. Particularly for small to mid-sized retirement plans, employers or other plan sponsors often use a bundled, full-service arrangement where custody of the plan assets, recordkeeping, and sometimes even retirement plan administration are all handled in-house by one provider.

From a consumer's perspective, they often engage with their retirement accounts primarily through the website of the plan's recordkeeper, who provides them information about their account balances, available investments, fees, and other plan information. These websites increasingly provide helpful tools to participants, including planning resources, financial education, and even advisory services for a fee. However, individual participants may seek tools and advice outside those provided by their plan – particularly investors who already have a relationship with an investment advisor who is not affiliated with their workplace-based retirement plan. To meet this demand, technology providers – from traditional banks to upstart fintech companies – increasingly enable consumers to use digital tools to engage in holistic financial planning and management.

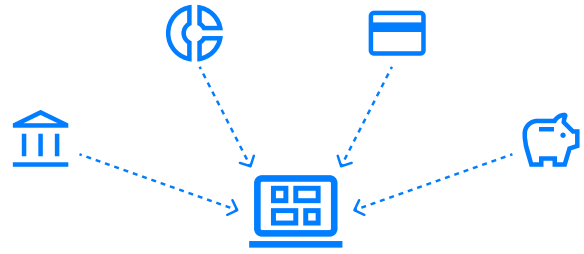


3 Consumers Routinely Authorize Digital Tools for Holistic Planning

In order to most effectively plan for retirement, consumers and their financial advisors need to consider not only the retirement savings they can expect to accumulate through their employment at one employer, but also other retirement accounts they may have, and their other assets (such as non-retirement plan savings and investments, real estate, and other holdings). Because consumers hold their financial information across many providers and platforms, the ability of digital tools to provide a comprehensive financial overview hinges on consumers authorizing financial advisors and other providers access to their financial accounts.

This process involves collecting financial information from various sources, such as bank accounts, investment portfolios, credit cards, and retirement plans, and consolidating it into a single, user-friendly interface. [According to FINRA](#), there are two primary methods through which authorized third parties aggregate retirement account data on behalf of consumers:

“To create a single dashboard, the aggregator will likely use one of two methods: an application programming interface (API), which offers a prearranged agreement to transfer data from the financial institution to the aggregator, or screen scraping, in which you provide your login credentials for each financial account so the aggregator can access that data.”



Leading financial planning and wealth management platforms, including [Morningstar](#), [Yodlee](#), and robo-advisors like [Wealthfront](#), routinely utilize data aggregation to serve their clients. Even major financial institutions such as [JP Morgan Chase](#) offer features that allow customers to link and view external accounts using data aggregation technologies. Without such capabilities, these platforms would be severely limited in their ability to offer consumers truly holistic and meaningful financial advice and planning.

The paramount importance of this aggregated, 360-degree view of financial information cannot be overstated. Financial advisors, for instance, may struggle to effectively fulfill their fiduciary duty to act in their clients' best interests without a complete understanding of their clients' integrated financial picture. This often necessitates access to 401(k) and other retirement savings data, which frequently remains outside the direct purview of a client's primary financial advisor, since it is held with the recordkeeper or the plan administrator. The fundamental basis of these tools is consumer authorization, meaning consumers consent to these technologies' ability to access their accounts in order to provide them a valuable service.

4 Custodians and Recordkeepers Also Offer Consumer-Authorized Tools

A critical point often overlooked in discussions around consumer-permissioned 401(k) and other retirement plan data access is that custodians and recordkeepers themselves frequently employ data aggregation as part of their own services. In fact, the Securities Industry and Financial Markets

Association – a trade organization representing asset managers – has published [Data Aggregation Principles](#), which “strive to provide customers with secure access to their financial information, while maintaining the security and integrity of our members' systems.”

Consider the following examples:

- **Fidelity Full View and eMoneyAdvisor:** Fidelity, one of the largest custodians and recordkeepers, provides its customers Full View, and advisors eMoneyAdvisor, each of which incorporate data aggregation to help individual investors fully understand their finances.
- **UBS My Total Picture:** UBS offers a feature called "My Total Picture" within its online services, which allows clients to view and track balances from their accounts held at other institutions, alongside their UBS accounts.
- **TIAA 360° Financial View:** TIAA offers a feature called 360° Financial View that enables participants to aggregate their financial information from "over 17,000" other financial institutions.
- **Charles Schwab Schwab Alliance:** Charles Schwab provides a client-facing website called Schwab Alliance that includes an aggregation feature, where clients "will need to provide their non-Schwab site credentials directly to Schwab's Aggregation Services provider."
- **JP Morgan Chase How to Link External Accounts:** JP Morgan Chase offers features allowing its customers to link external bank and investment accounts to their online banking portal. The underlying technology for this account linking often involves credentials-based aggregation, similar to how independent financial planning tools operate.

These institutions understand that consumers benefit from the ability to consolidate their financial information in one place, and provide cybersecurity to protect consumers, even in cases where they or their service providers may need to use client

credentials to access held-away accounts. To be clear, credentials-based access is a necessary and commonly accepted mechanism for data sharing, provided it is managed securely and consumers are protected in the process.

5 Consumer-Authorized Technologies Can be Consistent with Regulatory Requirements

As stewards of sensitive financial information, custodians and recordkeepers bear a fundamental responsibility for maintaining robust cybersecurity measures to protect consumer data. This responsibility encompasses safeguarding against unauthorized access, data breaches, and other cyber threats. As a result, custodians and recordkeepers have been historically cautious in their approach to consumer-authorized technologies. However, trends in cybersecurity and technology have shown that **custodians and recordkeepers can achieve and enhance cybersecurity while simultaneously supporting consumers' ability to benefit from services outside their systems.**

EBSA – the federal agency that I led – has regulatory and enforcement oversight over the millions of job-based retirement, health and other benefit plans covering more than 150 million Americans working for private employers.

Recognizing the trillions of dollars held by these employee benefit plans and their service providers, as well as the vast amount of personally identifiable data of participants and beneficiaries held and transferred by these plans and service providers, EBSA knew that, in today's digital threat landscape, retirement and health plans have become high-value honeypots - rich in sensitive data, lightly defended, and often overlooked in enterprise-wide cybersecurity strategies.

To address this issue, in 2021, EBSA issued its [Cybersecurity Program Best Practices](#), as well as [Tips for Hiring a Service Provider with Strong Security Practices](#) and [Online Security Tips](#). Under my direction, in 2024, EBSA [updated](#) those resources to provide additional assistance for ERISA retirement, health and other plans, sponsors, administrators, fiduciaries and their service providers.

These best practices include:

- Having a formal, well documented cybersecurity program;
- Conducting prudent annual risk assessments;
- Having a reliable annual third party audit of security controls;
- Clearly defining and assigning information security roles and responsibilities;
- Having strong access control procedures;
- Ensuring that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments;
- Conducting periodic cybersecurity awareness training;
- Implementing and managing a secure system development life cycle (SDLC) program;
- Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response;
- Encrypting sensitive data, stored and in transit;
- Implementing strong technical controls in accordance with best security practices; and
- Appropriately responding to any past cybersecurity incidents.

Cybersecurity is of utmost importance – this is what motivated EBSA to publish its guidance. EBSA's guidance recognizes that the use and transfer of data is a necessary part of the normal operations and administration of employee benefit plans. The guidance provides information and tools for plan fiduciaries to consider and use to safeguard benefits and data and comply with their ERISA fiduciary

duties. In following these standards and guidance, custodians' and recordkeepers' cybersecurity postures can be consistent with enabling customers to access and share their financial information in a prudent manner, while at the same time recognizing that it is an imperative to innovate and collaborate to provide secure, consumer-centric solutions that enable a holistic approach to financial planning.

6 Recommendations for a Consumer-Centric Retirement Planning Ecosystem

- 1. Plan Sponsors should understand the benefits these tools can deliver to participants, and the fiduciary implications therein:** The decision to provide their financial advisor with access to, visibility into, or management of their 401(k) or other retirement account lies with the plan participant or beneficiary, and involves a relationship between the advisor and retirement saver outside of the plan. Plan sponsors should, however, learn about these technologies and the improved retirement outcomes and customer service experience their participants and beneficiaries could enjoy if these technologies are made available in a secure and appropriate manner. Plan sponsors should ask their recordkeepers or other service providers whether they have considered using consumer-authorized

data aggregation tools. The DOL routinely focuses on the distinction between investor education and investment advice, and between services provided by the plan and those provided by third-parties outside of the plan in a separate relationship between the service provider and the participant or beneficiary. Consumer-authorized services like those discussed in this paper generally fall under the category of these outside third-party services, due to the fact that they are not provided by or through the plan service provider holding the assets, but by the third-party servicing the consumer. The DOL has long acknowledged that individual participants may seek guidance and advice from third-parties that are not affiliated with their workplace-based plans, and published

[Interpretative Bulletin 1996-1](#) to address the fiduciary implications of those activities.

2. Recordkeepers should explore partnering with third-parties to promote consumer outcomes:

While partnership is not necessary to facilitate consumer-authorized technologies, recordkeepers have a significant opportunity to actively foster a secure and open financial ecosystem by considering partnerships with companies enabling these services. Reputable data aggregators and financial technology providers implement robust security protocols, including encryption, multi-factor authentication, and strict data privacy practices, to protect consumer information. The focus should be on secure implementation and transparent practices. As FINRA's "Know Before You Share" guidelines suggest, and EBSA's cybersecurity guidance reinforces, the emphasis should be on consumer awareness and due diligence when sharing information, and on the responsibilities for safeguarding data. Recordkeepers can collaborate with fintechs to deliver value to customers, and ensure continued quality of service, provided that cybersecurity protections are in place.

3. Financial advisers should consider their fiduciary duties when using these consumer-authorized tools.

Trusted financial advisors are generally obligated to comply with fiduciary responsibilities to act in their clients' best interests. Critical to these decisions is evaluating the risks associated with products and technologies, and ensuring the benefits of those services are conveyed to the investor, while risks associated with those products are mitigated and disclosed. With proper consideration, consumer-permissioned access to 401(k) and other retirement accounts, facilitated by secure data aggregation tools, is a

vital component of holistic, meaningful, modern financial planning. It empowers consumers to take control of their financial destiny and enables advisors to fulfill their fiduciary duties more effectively. While promoting cybersecurity to protect client information, our collective focus should be on promoting secure data practices and ensuring that consumers remain at the center of their financial decision-making, with the freedom to share their data securely with trusted advisors and tools in a way that is secure and serves their long-term financial security.

4. Regulators should understand these technologies and encourage the safe development of tools that can help consumers improve their finances, including by publishing best practices.

Regulators at the state and federal level should take the time to fully understand these technologies and how they can benefit consumers. They should also consider any potential risks or concerns with these platforms, and ensure consumers understand those risks before using them. States like [Delaware](#) and [Texas](#) have taken an investor-focused approach, to ensure everyday consumers are equipped to make informed decisions that benefit their financial lives. Importantly, there are competitive considerations when consumers choose to use third-party services that may also be offered by their financial institution, such as advisory services. Retirement is a complex regulatory domain, with plans overseen by the DOL and advisors regulated by states or the SEC. Regulators should independently evaluate whether there need to be best practices in place for the regulated community, and what guidance and education can be provided to participants and beneficiaries regarding data aggregation.