



# Keeping Retirement Plans Secure in an Insecure World






# Keeping Retirement Plans Secure in an Insecure World


**Authors** Alison Salka  
Senior Vice President and Director  
LIMRA

Eric Sondergeld  
Independent Strategy Consultant and Researcher

**Sponsors** Aging and Retirement Strategic  
Research Program Steering  
Committee

 **Give us your feedback!**  
Take a short survey on this report.

[Click Here](#)



#### **Caveat and Disclaimer**

The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the Society of Actuaries Research Institute, Society of Actuaries, or its members. The Society of Actuaries Research Institute makes no representation or warranty to the accuracy of the information.

Copyright © 2022 by the Society of Actuaries Research Institute. All rights reserved.

# CONTENTS

- Executive Summary ..... 4**
  - Trends ..... 4
  - Targets ..... 4
  - Protecting Participants ..... 4
- Introduction ..... 6**
- The Evolution of Fraud ..... 6**
- Fraud Targets..... 7**
- The Balancing Act in Protecting Participant Accounts ..... 7**
  - Multi-factor authentication (MFA)..... 7
  - Rules for Distributions ..... 8
  - Eligibility..... 8
  - Where distributions are sent..... 8
  - Human involvement..... 8
  - Behind the scenes monitoring & investigation ..... 8
  - Use of Third-Party Vendors ..... 9
- The Role of Participants in Protecting Accounts ..... 9**
  - Account Protection Programs ..... 10
  - Cybersecurity..... 11
  - Attacks aimed at plan sponsors..... 11
  - Attacks aimed at the recordkeeper ..... 11
  - Industry best practices for cybersecurity and fraud ..... 12
- Concerns for the Future..... 12**
  - Fraudster sophistication ..... 12
  - Risks to the balancing act ..... 13
  - “Ware” attacks..... 13
  - Other concerns..... 13
- Methodology ..... 13**
- Acknowledgments ..... 15**
- List of Participating Companies ..... 16**
- About The Society of Actuaries Research Institute..... 17**
- About Secure Retirement Institute® ..... 18**

# Keeping Retirement Plans Secure in an Insecure World

## Executive Summary

In recent years, fraudulent actors have increasingly targeted participant balances in retirement plans. Activity jumped in 2016 and 2017, according to the interviews with 17 retirement plan recordkeepers and 6 subject matter experts who were interviewed for this study.<sup>1</sup> Recordkeepers generally report that their mitigation actions have been effective and that successful fraud attacks have decreased. However, in light of the increasing sophistication of fraudulent actors and the amount of money and trust at stake they recognize they must continue to build ever stronger defenses as the fraud landscape continues to evolve.

### TRENDS

Cyber organized crime is growing. Fraudsters have been relatively successful gaining access to information and will likely become more sophisticated in their use of it. Entire organizations are in business to commit fraud.

In previous years, fraud efforts were commonly directed at call centers. The increased ability to do business online, including requesting distributions, means that fraudsters can avoid the scrutiny of speaking with people.

As recordkeepers continue to add digital capabilities to increase convenience, they strive to ensure they are not creating another path for fraudsters to access accounts.

### TARGETS

About half of the recordkeepers mentioned that executives, as well as participants with higher balances or higher compensation are frequent targets. These people are relatively easy to research online.

A number of recordkeepers noted that the healthcare sector – from medical practices to hospitals – are frequent targets.

Many attacks against participant accounts are precipitated by a breach at their employer. For this reason, recordkeepers recognize the importance of good communication between them and plan sponsors when breaches occur at either organization.

### PROTECTING PARTICIPANTS

Implementing robust fraud prevention controls without overly burdening participants is a priority for recordkeepers.

Multifactor authentication seems universal and is often mandatory.

---

<sup>1</sup>See the Methodology section for definitions and for the types of experts interviewed for this study.

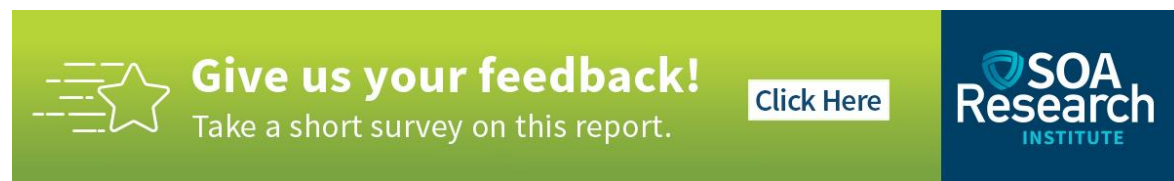
Recordkeepers tend to have their strictest controls around the ability to perform sensitive transactions, especially distributions.


Recordkeepers are building proactive reporting and analytics programs to identify red flags and suspicious activity. The analytics may be rules-based and/or behavioral.


Recordkeepers consider fraud protection a team effort. They ask plan sponsors and participants to contribute to the effort. With respect to participants, recordkeepers educate and communicate through a variety of channels.

Some recordkeepers offer a protection program that reimburses participant losses if an account is breached through no fault of the participant. This is usually contingent on the participant following a specific set of actions to protect their account on an ongoing basis.

Most recordkeepers report that their organization has cyber insurance, though it's not always clear what specific protection the insurance provides retirement plans.



 **Give us your feedback!**  
Take a short survey on this report. [Click Here](#)



## Introduction

In recent years, fraudulent actors have increasingly targeted participant balances in retirement plans. The industry quickly took note and action to prevent successful fraudulent attempts.

Plan sponsors and participants entrust recordkeepers with their plan assets, and recordkeepers – with reputations as being safe places to administer retirement plans on the line – are intent on protecting these assets.

LIMRA’s Secure Retirement Institute and the Society of Actuaries Research Institute Aging and Retirement Strategic Research Program collaborated on this report to assess the current situation through a series of interviews among 17 retirement plan recordkeepers and 6 subject matter experts regarding industry practices in financial crimes and fraud prevention.

## The Evolution of Fraud

Recordkeepers interviewed generally say retirement fraud became an issue sometime in the past few years, with several citing 2016 or 2017 as when they were first attacked or saw a marked increase in attacks. While the number of fraudulent attempts may have increased or decreased since then at any particular recordkeeper, the number of *successful* attempts has significantly decreased to a minimal amount. The lessons of the past made recordkeepers hyper-vigilant and retirement plan fraud remains a significant concern among all interviewed.

There are several explanations for the decline in *successful* fraud. Most credit the implementation of operational controls to detect and combat fraud. Others suggest that fraudsters simply go where the money is, especially where the money is easiest to access. Some suggested fraudsters began by attacking the banking and credit industries until controls making it more difficult to commit fraud against them were implemented. Retirement plans (and insurance company products such as life insurance and annuities) became the next targets. Then those organizations implemented significant controls to protect participant accounts, forcing fraudsters to consider their next victims. Fraudsters may have found them during the COVID-19 pandemic and set their sights on accessing federal (stimulus checks, Paycheck Protection Program (PPP) loans, etc.) and state (unemployment insurance) programs. Some reported that 2020 and the first half of 2021 have been uncharacteristically quiet from a fraud perspective but express concern that things could change as pandemic-related programs conclude.

Company experience varies regarding the source of fraud. For some, it’s primarily known-party, or familial, fraud. Because family members often have access, whether legitimately or not, to a participant’s information and even to their digital devices, they can appear to be legitimate in the eyes of the recordkeeper. The good news is that when familial fraud is detected, it is relatively less difficult to recover the funds and/or to prevent continued fraud. For other companies, third party fraud has become the dominant source of threats, though even for these firms, known party fraud continues.

There has also been a shift from fraudsters committing fraud by phone to call centers to committing fraud that exploits online accounts. Historically, fraudsters would often contact call centers “phishing” for information in the hope of gathering enough of it to commit fraud. With the increasing ability to do business online (including requesting distributions), fraudsters can leverage data and not have to speak with anyone.

The level of fraudster sophistication continues to increase. Many efforts at fraud have evolved into organized enterprises, investing in modern technological infrastructure such as artificial intelligence and cloud-based computing and storage. It appears that, so far, they are better at obtaining information about plan participants than actually exploiting it. However, once they have enough information to steal someone’s identity, they go after whatever assets that individual owns, including retirement plan assets. Identity theft is increasing rapidly, especially as related to security accounts, where retirement plan fraud is likeliest be reported.

## Fraud Targets

Many recordkeepers do not discern any particular pattern in the types of plans, employers, participants, etc. targeted by fraudsters. However, those offering both defined benefit and defined contribution plans see very little fraudulent activity in the former and most in the latter.

About half of the recordkeepers mentioned that participants with higher balances, and/or earning higher compensation, are often targeted, as are executives. These individuals are relatively easy to research online. Biographies, and in some cases salaries, are publicly available. Targeting these individuals is sometimes referred to as *spearfishing* or *whaling*. Although fraudsters hope to capture large distributions, they often have no idea how large or small a balance an individual participant's account has. As a result, many participant accounts with small balances end up becoming targets.

About one third of recordkeepers mentioned plans in the healthcare sector – ranging from medical practices to hospitals – as frequent targets of fraud. Participants in these plans would include doctors, who usually earn a good living and could be the primary targets.

Other industry sectors mentioned include education, retail, and manufacturing. The latter may be less inclined to set up an online account. Retirees are also sometimes targeted due to their higher account balances and the fact that they are often less engaged with or proficient in the use of technology.

## The Balancing Act in Protecting Participant Accounts

Protecting participant accounts from fraud is obviously critically important to recordkeepers. So is providing a good customer experience. As recordkeepers consider incorporating various fraud prevention controls, they strive to implement them in a way that is not overly burdensome on participants. This section summarizes some of the ways recordkeepers are employing people, processes, and technology to prevent fraud.

### MULTI-FACTOR AUTHENTICATION (MFA)

The best way to protect participant accounts is to ensure that anyone calling the recordkeeper or logging into the participant website is who they purport to be. Using multiple factors to authenticate a participant's identity is now universally employed and in most cases is considered mandatory. These factors may include:

- The IP address of the device being used.
- Geographic location.
- Participant behavior (e.g., time of day, frequency of access).
- One-time passcodes (OTP) sent to the participant's email or mobile device. Several recordkeepers mentioned a preference (or even restriction) for sending OTPs to a mobile device as they are more difficult to hijack than email addresses.
- Biometrics such as voice recognition, facial recognition, or fingerprint.
- Knowledge-based authentication, where the recordkeeper will ask about vehicles owned, addresses, relatives, etc. One challenge with knowledge-based questions is some answers may be discoverable via social media or hacked data from credit monitoring companies.
- Use of third-party authenticator apps.
- Device "fingerprinting," by uniquely combining multiple characteristics about a device. Whether using fingerprinting or IP address, recordkeepers may challenge logins coming from a device they have not seen before.

Some recordkeepers are developing methods that are not consistent as regards the factors they gather for authentication, making it more difficult for fraudsters to gain access to an account. Recordkeepers may also repeat the authentication process beyond login for certain sensitive transactions, such as loans and distributions.

## RULES FOR DISTRIBUTIONS

The true test of an antifraud program is its ability to permit only authorized distributions and other sensitive appropriate transactions. As a result, recordkeepers tend to have their strictest controls around the ability to perform these transactions. These controls tend to fall into three categories: those on eligibility, those on destination, and those that require that real people be involved in the process.

## ELIGIBILITY

Many recordkeepers will place a temporary hold on distributions from accounts that have had recent changes, such as to the participant's address or bank account. The minimum time permitted between these changes and distribution eligibility can range from 7 to 30 days. This practice allows time for notifications of these changes to be sent to the participant in case they did not make the change.

## WHERE DISTRIBUTIONS ARE SENT

Some recordkeepers will only send distributions to the participant's address of record and not to an advisor or another third party. They may first send a form to the participant's address to be completed and returned before a distribution is processed. While a growing number of recordkeepers allow online distribution requests, they still may mail a paper check to the participant.

Recordkeepers allowing electronic distributions often use vendors which can verify whether the participant actually owns the destination account. One recordkeeper that does electronic distributions has a limit of \$5,000 on any ACH transfers.

## HUMAN INVOLVEMENT

Several recordkeepers mentioned inserting real persons into the distribution process as an additional control. Some of the methods employed include:

- Referring participants to the plan sponsor when making a distribution request (or to change their PIN, email or mailing address).
- Mailing a distribution form to the participant's address of record (as mentioned above).
- Calling participants following some online distribution requests to confirm they initiated the transaction.
- Having a real person review all distribution requests before they are released.

## BEHIND THE SCENES MONITORING & INVESTIGATION

In addition to specific controls and procedures to prevent and deter fraud, recordkeepers have built proactive reporting and analytics programs to develop red flags and monitor suspicious activity. The analytics may be rules-based and/or behavioral. For example, behavioral analytics determine patterns of how, when, or from where a participant may interact with the participant website or call center/Interactive Voice Response (IVR) system. They also typically scrutinize accounts that have had sensitive transactions such as changes to passwords, addresses, or banking information. They watch for fraudsters' techniques such as bot attacks or credential stuffing, where a hacker writes a script to bombard potentially thousands of financial services organizations to test customer credentials.



Regardless of the source of potentially suspicious activity, recordkeepers may decide to place an alert on an account or plan, freeze accounts, force a password reset, or even contact the participant to determine whether the activity was legitimate. They may also do these things at the request of a plan sponsor or participant reporting related suspicious activity (e.g., a participant who was victim of identity theft).

Suspicious activity is typically then reviewed by a fraud investigative team. These teams tend to err on the side of caution, which results in a high percentage of investigations revealing legitimate activity on the part of plan participants.

## USE OF THIRD-PARTY VENDORS

Recordkeepers subscribe to vendor services to help combat fraud as well as to minimize friction when participants call in or login. Table 1 below lists those receiving mentions from multiple recordkeepers. The list below is in no way intended to imply an endorsement of any of these products by the authors or sponsoring organizations of this report. The full set of services/vendors used is likely much longer.

**Table 1**  
**VENDORS RECEIVING MULTIPLE MENTIONS**

Vendor	Service
LexisNexis	<i>PhoneFinder</i> helps contact centers understand the likelihood that a caller is associated with a particular phone number.  <i>ThreatMetrix</i> provides digital identity intelligence for account setup, account logins, and distribution management.
Pindrop	Offers a variety of fraud prevention and authentication solutions that monitor calls to the IVR and contact center for voice, device, and behavior, and deliver a variety of risk scores to the call center representative.
GIACT	Confirms in real-time whether a participant actually owns the bank account designated for a distribution.
Neustar	Validates phone numbers on incoming calls.
LIMRA/LOMA	FraudShare is an industry-wide fraud information sharing platform.

\*Note that the full breadth of solutions from these organizations are not included here.

## The Role of Participants in Protecting Accounts

Recordkeepers consider fraud protection a team effort. They do their part to protect participant accounts, but they also look for plan sponsors and participants to contribute to the effort. They mainly do this by educating and communicating with participants through a variety of channels. These may include seminars, newsletters, email campaigns, information on the participant website, and other means. Often the plan sponsor needs to agree to participate in these communications.

First, recordkeepers usually encourage participants to register for an online account, which includes setting up multi-factor authentication, formulating security questions and providing contact information (such as email address and phone number). Participants are urged to select security questions whose answers are not discoverable on

social media and to not share the answers with anyone. Setting up their online accounts means that fraudsters are not able to impersonate a participant and set up an account.

Recordkeepers then offer numerous suggestions for how participants can safeguard their accounts. This may include recommendations to review quarterly statements or to log onto the participant website frequently. This advice may appear contrary to the “set it and forget it” advice participants often receive regarding asset allocation and investing in general. Recordkeepers may also suggest participants keep their contact information current and protect their devices and their identities. One recordkeeper allows participants in some plans to put a voluntary lock on their account to disallow distributions.

Using technology to protect accounts is very efficient. However, not all participants may have access to a computer or have the ability to effectively manage and protect their accounts. Recordkeepers employ a variety of methods to support these participants. For those with limited access to a computer, recordkeepers may resort to using paper forms for transactions, providing service via telephone (perhaps using knowledge-based questions), or involving the plan sponsor. In cases where the recordkeeper is aware of a participant with cognitive decline, many have processes to authorize a “trusted” person to access the account on the participant’s behalf.

### ACCOUNT PROTECTION PROGRAMS

Another way to encourage participants to do their part in protecting their accounts is by offering a protection program. These programs reimburse participant losses if their account is breached through no fault of their own, provided the participant follows a prescribed list of actions to protect their account on an ongoing basis. Seven of the 17 recordkeepers interviewed mentioned they offer such programs. However, many do not. Those who do not are of the opinion that many protection programs have so much fine print that the benefits will rarely be triggered. Some of these recordkeepers also recognize the optics of not offering such a program when trying to sell new plans and are therefore considering adding one. In the end, most feel that having or not having a program does not change the end result. Regardless of the existence of a program, virtually all recordkeepers review every case and have often decided to make the participant whole, at least at this stage of industry development. When it comes to protecting participant accounts, a real benefit of these programs is the encouragement they can provide for participants to take the necessary steps to protect their accounts.

A review of six recordkeepers’ account protection programs confirms much of the above sentiment. All six describe when they will reimburse as well as when they won’t. They do provide a list of steps that participants need to take on an ongoing basis for any claim they file to be reimbursed. The number of steps varies from a handful to many (which may be the source of the presumed fine print). The following are steps that participants must take that are included in all six reviewed programs:

- Keep contact information current, usually by including a mobile number for receiving text alerts from the recordkeeper.
- Regularly review their accounts for accuracy and suspicious activity. Only one recordkeeper defines “regularly” (e.g., every month).
- Update the security software on the device(s) used to access their accounts.
- Do not share their login credentials or security questions with anyone.
- Alert the recordkeeper either immediately or in a timely manner of any suspicious activity on their accounts. “Timely” was also not always defined; when it was, it ranged from 1 business day to 90 days.

The requirements generally fall into two categories. The first are related to the participant website (e.g., choosing to receive text notifications, enabling security questions or multi-factor authentication). The second are common sense practices people should follow in their digital lives. Finally, just one program included steps the plan sponsor must take for the program to qualify.

## CYBERSECURITY

Accenture reports that cyber intrusion activity around the world increased 125% in the first half of 2021 when compared to the same time in 2020.<sup>2</sup> This jump was mostly caused by “web shell activity ... targeted ransomware and extortion operations, and supply chain intrusions.” Three nations comprised most of the incident volume: the United States (36%), the United Kingdom (24%), and Australia (11%). BenefitsPRO cites an IBM Security global survey finding that data breaches cost companies an average \$4.24 million per incident (a record high).<sup>3</sup> The article suggests that the rapid move to remote work during the pandemic is a contributing factor. Taking a broader view, a McKinsey study concluded that, although companies across industries are progressing in their cybersecurity efforts, “most organizations in all industries have much yet to do to protect their information assets against threats and attacks.”<sup>4</sup>

Cyberattacks seek to collect information that can be leveraged for profit. In retirement plans, those attacks can be aimed at the recordkeeper, third party administrator, plan advisor, plan sponsor or participant. As discussed above, recordkeepers recommend participants protect their devices, identities, and otherwise not share answers to knowledge-based questions on social media.

## ATTACKS AIMED AT PLAN SPONSORS

Many attacks against participant accounts are precipitated by a breach at their employer. For this reason, recordkeepers recognize the importance of good communication between them and plan sponsors when breaches occur at either organization. While a few recordkeepers interviewed *require* or are planning to require (through service agreement language) plan sponsors to notify them if they have been breached or a victim of a ransomware attack, most do not. The latter, however, *ask* plan sponsors to notify them if such an event were to happen. Most recordkeepers reported that plan sponsors often volunteer this information. The difficulty is that not all breaches of plan sponsors reveal sensitive information regarding plan participants, so the plan sponsor needs to make a judgment call. Plan sponsors are also dealing with an emergency situation and may not initially think of implications to the retirement plan. Some recordkeepers will reach out to plan sponsors if they learn through other means they were breached. Similarly, one recordkeeper mentions they take precautionary steps with the accounts of participants they learn were victims of identity theft.

## ATTACKS AIMED AT THE RECORDKEEPER

Despite the controls recordkeepers put in place to protect participant accounts, cyber breaches are still possible. For that reason, it can be beneficial to have insurance to cover such instances. Most recordkeepers report that their organization has cyber insurance, though it is not always clear what specific protection it provides retirement plans, especially since a) the language in these policies needs to be specific and b) these policies are typically purchased at the corporate level and cover the broader business and not solely the retirement plans business. A few recordkeepers have purchased fidelity bonds, a type of crime insurance. These typically include a high deductible on a per occurrence basis, to the degree that the benefits are rarely triggered. As a result, many recordkeepers end up self-insuring much of their fraud risk.

Cybersecurity and fraud questions have become standard practice in requests for proposals (RFPs) when recordkeepers are selling new plans. Recordkeepers report that most, if not all, RFPs include them. Similarly, these topics are commonly covered in annual reviews with plan sponsors. Recordkeepers see these meetings as

---

<sup>2</sup>Accenture’s Cyber Incident Response Update, Accenture, 2021.

<sup>3</sup>2020’s rapid shift to working from home upped the cost of data breaches, BenefitsPRO, August 4, 2021.

<sup>4</sup>Organizational cyber maturity: A survey of industries, McKinsey & Company, April 4, 2021.

opportunities for the recordkeeper to educate plan sponsors about the importance of having cyber insurance to protect their business and to remind those who already have it to understand whether the protection includes the retirement plan.

## INDUSTRY BEST PRACTICES FOR CYBERSECURITY AND FRAUD

This year, two organizations released recommended best practices for protecting retirement plans from cybersecurity attacks and fraud, including advice for plan sponsors, participant, and recordkeepers

In April 2021, the Employee Benefits Security Administration of the U.S. Department of Labor (DOL) issued<sup>5</sup>:

- *Tips for Hiring a Service Provider with Strong Cybersecurity Practices,*
- *Online Security Tips* for participants and beneficiaries, and
- *A set of twelve Cybersecurity Program Best Practices* for recordkeepers.

In July 2021, the SPARK Institute and its Data Security Oversight Board published a set of seven Industry Best Practice Fraud Controls.<sup>6</sup> Each control objective provides guidance for plan sponsors, participants, and recordkeepers. One covers customer reimbursement policies, which are described earlier in this report as account protection programs.

All recordkeepers interviewed maintained that their controls meet or exceed the DOL's best practices. Several have written marketing materials, white papers, or press releases to demonstrate their compliance with them.

Few recordkeepers offered suggestions for best practices beyond the DOL's recommendations. Some noted that the DOL's focus was on cybersecurity and not fraud specifically. Additional best practices offered include:

- Customer guarantees (included in the SPARK Institute's best practices).
- Putting a hold on all participant's accounts when they normally would not be taking a distribution (e.g., prior to retirement age).
- Developing an industry standard for multifactor authentication.
- Frequent communication with participants to keep their contact information current.
- Employing anomalous behavior detection.

## Concerns for the Future

Although recordkeepers generally report that the number of successful fraud attacks has significantly decreased, they understand that their success is a result of many factors both within and beyond their control. They also recognize they must remain vigilant as the fraud landscape continues to evolve.

## FRAUDSTER SOPHISTICATION

Recordkeepers' primary concern is to ensure that the person they are talking to (or the person trying to access the participant website) is who they claim to be. Organizations committing fraud will become increasingly sophisticated in their efforts, whether through leveraging data and technology or social engineering. Some observers feel that

---

<sup>5</sup>US Department Of Labor Announces New Cybersecurity Guidance For Plan Sponsors, Plan Fiduciaries, Record-Keepers, Plan Participants, April 14, 2021.

<sup>6</sup>Retirement Industry Leaders Define Best Practices to Defeat Retirement Account Fraud, July 21, 2021.

fraudsters have been relatively successful gaining access to information and will become more sophisticated in their use of it. There is also the concern that fraudsters will be able to leverage all the data that's been breached over the years from credit companies and credit monitoring services. Perhaps most concerning is that there are now entire organizations whose full-time business is to commit fraud, falling under the category of cyber-organized crime.

### RISKS TO THE BALANCING ACT

As mentioned earlier, recordkeepers seek to balance the security of participant accounts with the experience offered to participants. As recordkeepers continue to add digital capabilities to increase convenience, they strive to prevent the inadvertent creation of another path for fraudsters to access accounts.

### “WARE” ATTACKS

Some recordkeepers are most concerned with new forms of financial services malware or ransomware. A recordkeeper can be doing all the right things to protect participant assets, but all it takes is one successful attack to cause great harm. This could happen at either the recordkeeper or plan sponsor level.

### OTHER CONCERNS

Recordkeepers expressed a wide variety of additional concerns for the future. These include:

- Vulnerability from partners or other service providers who have access to participant data.
- How to get participants to register for an online account, where protections are stronger because they set up additional authentication.
- Fraudsters figuring out a way to enroll a nonparticipant in the plan and then withdraw the first contribution before the employee is aware of what happened.
- Email hacking fraud. Some recordkeepers send one-time passcodes to emails and mobile phones, the latter currently considered more secure.
- Fraudsters returning their attention towards retirement plans as opportunities to commit PPP loan, federal stimulus check, and unemployment insurance fraud decrease.
- Fears that the current success in combatting fraud will not last forever.
- Variables out of their control.

## Methodology

There are many individuals and organizations involved in U.S. employer-sponsored retirement plans:

- Plan participant – the employee or former employee who is using the plan to help fund their retirement.
- Plan sponsor – the employer that is offering the plan.
- Advisor – the financial representative that matches employers (usually smaller and midsize employers) with retirement plan providers.
- Recordkeeper – an organization that keeps track of contributions, investments, participant balances, and administers loans and other distributions from the plan. The recordkeeper is often the provider of the retirement plan.

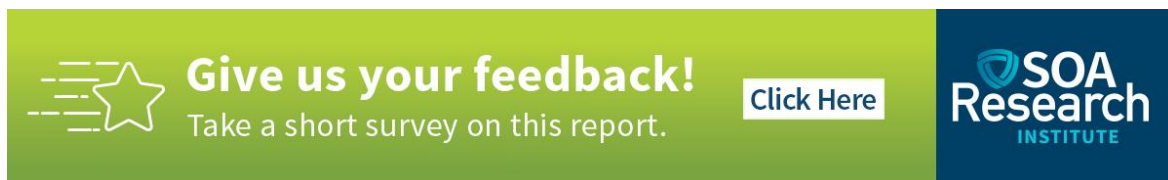
In June and July 2021 researchers conducted a series of 30-minute interviews with:


- Seventeen recordkeepers. Recordkeepers were selected to represent a range of size and breadth of types of plans offered. Collectively, these organizations represent 64% of U.S. defined contribution plan assets


and 54% of plans.<sup>7</sup> Those interviewed had titles ranging from manager to senior vice president, with director being most common and typically had oversight of areas such as fraud prevention, information security, and risk management.

- Six subject matter experts collectively representing perspectives of regulation, recordkeepers, plan sponsors, participants, and advisors.

Researchers also reviewed recordkeeper materials regarding guarantees and cyber security.

A horizontal banner with a green-to-blue gradient background. On the left is a white star icon with motion lines. To its right is the text "Give us your feedback!" in bold white font, followed by "Take a short survey on this report." in a smaller white font. Further right is a white rectangular button with the text "Click Here" in blue. On the far right is the SOA Research Institute logo, which consists of a blue shield icon followed by the text "SOA Research" in white and "INSTITUTE" in blue below it.

 **Give us your feedback!**  
Take a short survey on this report. [Click Here](#)

 SOA  
Research  
INSTITUTE

---

<sup>7</sup>Data as of 12/31/2020 and compiled from the 2021 Recordkeeping Survey, [www.plansponsor.com](http://www.plansponsor.com).

## Acknowledgments

The researchers' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the Project Oversight Group and others for their diligent work overseeing, reviewing and editing this report for accuracy and relevance.

Project Oversight Group members:

Paula Hogan

Jen Keefe

Cindy Levering

Sandy Mackenzie

Betty Meredith

Jonah Morales

Gary Mottola

Hector Ortiz

Anna Rappaport

Sara Rix

Faisal Siddiqi

Steve Vernon

At the Society of Actuaries Research Institute:

Steve Siegel, Sr. Research Actuary

Barbara Scott, Sr. Research Administrator

## List of Participating Companies

ADP Retirement Services

Alight Solutions

Ameritas

Ascensus

CUNA Mutual Retirement Solutions

Empower Retirement

Equitable

John Hancock

Lincoln Financial Group

Nationwide

Principal

Prudential Retirement

Schwab Retirement Plan Services, Inc.

Securian Financial

T. Rowe Price

TIAA

Voya Financial



## About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its [strategic research programs](#): aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of [topical research available](#), including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute  
475 N. Martingale Road, Suite 600  
Schaumburg, Illinois 60173  
[www.SOA.org](http://www.SOA.org)

## About Secure Retirement Institute®

The Secure Retirement Institute® (SRI®) provides comprehensive, unbiased research and education about all aspects of the retirement industry to improve retirement readiness and promote retirement security. For information on the Secure Retirement Institute, visit: [www.limra.com/sri](http://www.limra.com/sri).