Six Easy Steps to Keep Your Plan Assets Safe

Joel Shapiro, JD, LLM, Senior Vice President, ERISA Compliance

Cyber fraud is a growing concern globally. Individuals are typically very careful to keep their bank account and email authentication information safe, but they aren't always smart with the rest of their personal information.

Participants need to be vigilant with their retirement savings accounts as well. In the past year we've seen a slew of cases of attempted fraud – some successful – against retirement savings plan participants across a multitude of recordkeepers. The good news is that virtually all recordkeepers view security as a prominent priority and diligently update their technology. However, their security can only go so far if the participant isn't being equally vigilant.

Educate your plan participants on the following tips to ensure the security of their retirement savings accounts.

1. Use all available levels of authentication. If your plan's recordkeeper comes out with a new type of authentication, your participants should implement it immediately.
2. If participants frequent a website or have an account with a company whose website and information has been compromised, they should change all of their passwords for all online accounts.

3. Remind participants to use strong passwords. Utilize letters, capitalization, numbers and symbols. Don't use recognizable words. Don't use the same password for multiple purposes. Have the password be at least 14

characters in length. Consider changing passwords frequently. Using a password manager can make this task less unwieldly.

4. Don't send authentication information to any third parties, and remind participants to limit authentication access to use on sites which are navigated to independently – not through a link or other prompt.
5. Check your participants' accounts frequently and address any irregularities, and remind participants to keep an eye out, too.
6. Ask participants to immediately contact you if they receive any "updates" that look suspicious so you can notify your recordkeeper.

Keep your participants in the know. We recommend sending them the participant memo that is included with this

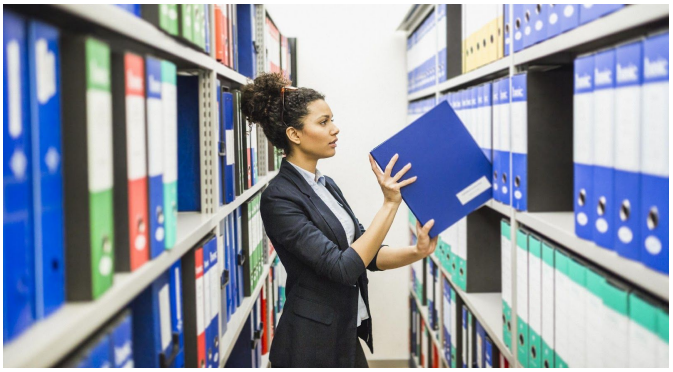
newsletter on the importance of remaining vigilant when it comes to cybersecurity – it's one of the most important investments your participants can make.

For more information on keeping your plan assets safe from cyberattack, please contact your plan advisor.

About the Author, Joel Shapiro, JD, LLM
As a former practicing ERISA attorney Joel works to ensure that plan sponsors stay fully informed on all legislative and regulatory matters. Joel earned his Bachelor of Arts from Tufts University and his Juris Doctor from Washington College of Law at the American University.

Records and Their Expiration Dates

"What records should I keep? How long should I keep them? How should I organize my files?"



Advisors have been asked these questions time and time again by plan sponsors looking for a general guideline for record expiration dates.

Record retention doesn't need to be a mystery, and the filing system doesn't need to become a tomb. For audits, remember the following requirements.*

Documentation	Retention Requirement for Audit Purposes
Plan Documents (including Basic Plan Document, Adoption Agreement, Amendments, Summary Plan Descriptions, and Summary of Material Modifications)	At least six years following plan termination
Annual Filings (including 5500, Summary Annual Reports, plan audits, distribution records and supporting materials for contributions and testing)	At least six years
Participant Records (including enrollment, beneficiary, and distribution forms; QDROs)	At least six years after the participant's termination
Loan Records	At least six years after the loan is paid off
Retirement / Investment Committee **meeting materials** and notes	At least six years following plan termination

As for organizing your fiduciary file, we suggest a format that includes the following sections:

Documents with all plan documents, amendments, tax filings and so on.

Administrative for all audit results, contribution records, Fiduciary Plan Review meeting minutes, fee benchmarkings, participant complaints.

Participant Communication containing copies of enrollment materials, communications and memos, and meeting sign-in sheets.

Investments with a listing of fund menu with expenses, Fiduciary Investment Review meeting minutes.

If a participant, auditor, or DOL agent requested plan information, could you find it quickly? The key is twofold: keep the things you need and store them so you can find them easily.

Of course, these are only general guidelines. For questions about your specific case, contact your plan advisor to discuss best practices for keeping records.

**For litigation purposes, we recommend that documents be retained indefinitely.*

Hey Joel! – *Answers from a recovering former practicing ERISA attorney*

Welcome to *Hey Joel*! This forum answers plan sponsor questions from all over the country by our in-house former practicing ERISA attorney.

Dear Anxious,

First, understand that we are all still awaiting further guidance from the IRS/Treasury on the new hardship safe harbor rules. The suspensions don't so much as "go away" as much as the necessity to suspend deferrals potentially becomes optional. That said, if a plan wants to keep the suspension, I believe they may do so. The only question would be whether or not the safe harbor remains intact for the plan sponsor. As originally stated, we are still waiting on additional guidance from the IRS/Treasury on whether or not all the new rules would be required, or are just optional, for the safe harbor protection.

Also Anxious,

Joel Shapiro

About the Author, Joel Shapiro, JD, LLM
As a former practicing ERISA attorney Joel works to ensure that plan sponsors stay fully informed on all legislative and regulatory matters. Joel earned his Bachelor of Arts from Tufts University and his Juris Doctor from Washington College of Law at the American University.

Participant Corner: Keep Your Plan Assets Safe!

This month's employee memo reminds participants to remain vigilant when it comes to the cybersecurity of their retirement plans. Download the memo from your Fiduciary Briefcase at fiduciarybriefcase.com and distribute to your participants. Please see an excerpt below.

You work hard for your money. You wisely choose to defer a portion of your salary for your interests in your retirement years. The plan is designed to help you grow your savings to an appropriate amount of money to support you once you reach your retirement years.

But as you are aware, the plan is only as effective as you make it. If you defer too little, or make unwise investment decisions there is a chance that you will not reach your goals. Similarly, if you drain your plan balance over the years, you understand you will find a shortfall in retirement. What many participants do not think about is being responsible for the security of their savings as well.

Cyber fraud has been a growing concern globally for years. Individuals are typically very careful to keep their security measures (passwords, authentication codes, etc.) private with regards to their banking and electronic mail accounts. However in the past few years there have been breaches of major companies containing personal information of individuals. And unfortunately much of the personal information has become accessible by bad actors on the dark web.

Participants need to be vigilant with their retirement savings accounts as well. In the past 12 months there have been a slew of cases of attempted fraud, some successful, enacted on retirement savings plan participants. And these attempts have occurred across a multitude of recordkeepers. The good news is that virtually all recordkeepers have security as a prominent priority and spend. They are constantly updating their security technology and protocols. But their security can only go so far if the participant is not being equally vigilant.

The following are a few prudent tips for participants in ensuring the security of their retirement savings accounts:

- Use multiple levels of security and authentication – if your plan's recordkeeper comes out with a new level/type of authentication, engage it immediately.
- If you frequent a website, or have an account with a company, whose website and information has been compromised, change all your passwords. For example, Yahoo recently had a large breach – a breach containing passwords – if you ever had a Yahoo account you should change your password.
- Make sure your password is strong – utilize letters, capitalization, numbers, and symbols. Don't use recognizable words. Don't use the same password for multiple purposes. Have the password be at least 14 characters in length. Consider changing your password on a frequent basis.
- Never send your authentication to anyone requesting it. It should be limited to use on sites on which you navigated to independently of any outside request.
- Check your account on a semi-regular basis for any irregularities.
- Immediately contact your plan administrator and/or the recordkeeper if you receive any update that sparks your concern – do not wait, the money could leave the U.S. quickly.

As your employer we are always looking out for your wellbeing. We trust that the plan is in good hands with our recordkeeper. We have reviewed their cyber security protocals and technology. But we felt a need to provide a gentle reminder that your involvement is crucial in maintaining the security of your account too.

We want your savings experience to be as simple and easy as possible. We want you to someday enjoy your retirement years.

individual situation.

To remove yourself from this list, or to add a colleague, please email us at JGILLEN@CambridgeSecure.com or 847-778-1522.

ACR#304542 12/18

A Proud Member of