# RETIREMENT PLAN PERSPECTIVES

Insights for Your Plan and Employees

Q2 2021

## Handle with Care: 401(k) Cybersecurity

Even casual followers of the news know that the safeguarding of personal and sensitive data is a serious matter. And although the most publicized cases of people's personal information being exposed are usually associated with big corporations, small businesses are by no means immune to information security breakdowns.

An increasingly central aspect of a retirement plan sponsor's fiduciary oversight is how they—and the service providers they contract with, such as recordkeepers or third-party administrators—protect employees' sensitive personal data. In the past, fiduciaries may have treated cybersecurity as an afterthought, but, especially with the Department of Labor recently casting a watchful eye, cybersecurity should be near the top of any retirement plan fiduciary's priority list.

### Why Do 401(k) Cybersecurity Breakdowns Occur?

First, it's helpful to become familiar with some of the most common reasons for cybersecurity breaches:

- **Lack of awareness.** Employees, whose job responsibilities require them to handle sensitive employee data, are often insufficiently trained on cybersecurity best practices. Investing in cybersecurity education is a worthwhile endeavor. Fortunately, there are several free resources and programs available to help train them to be the first line of defense.
- **Vendors and service providers have insufficient cybersecurity policies.** Remember, as a plan sponsor and fiduciary, among the most critical tasks you have are the prudent selection of service providers and the continuous monitoring of their performance, which includes their data security standards and protocols.
- **Cyberthieves look for every possible advantage.** Cyberthieves are increasingly clever, and they adapt to efforts to foil them at a lightning-fast pace. They frequently pose as people they aren't—such as a service provider, employee, or beneficiary—to gain access to personal data or funds. Further, cyberthieves often target the data of small businesses. Why? Because they typically lack the resources and technology infrastructure of larger businesses and are an easier mark for cyberthieves.

### Creating a Culture of Cybersecurity Awareness

What can business stakeholders and plan fiduciaries do to foster a culture of data security awareness? Here are three tips to help your organization stay ahead of cybersecurity threats:

1. **Establish a foundation of cybersecurity awareness within your organization.** Maintaining a steady, effective security awareness program helps employees who handle sensitive data make the right decisions to help keep your firm's information safe. Here are some ideas to incorporate into your data security awareness program:
   - Make changing passwords a task that is required regularly.
   - Offer rewards to employees who find ways to improve office cybersecurity.

**Handle with Care: 401(k) Cybersecurity** *(continued)*

- To promote accountability, implement a way for employees to anonymously report cybersecurity breaches that they witness.

> **DOL Announces Cybersecurity Guidance for Retirement Plan Fiduciaries**
>
> In April 2021, the Department of Labor provided new guidance to plan sponsors, plan fiduciaries, recordkeepers, and plan participants about cybersecurity best practices, including tips that will help fiduciaries protect participants and assets that may be at risk from both internal and external cybersecurity threats. Visit the Department of Labor website to learn more.

2. **Adopt 401(k) cybersecurity policies.** Policies should address all the security concerns and practices of your business's retirement plan. Store your policies in a place where your staff can read them, and review them annually to ensure that they're still relevant. Be sure the policies clearly address the roles and responsibilities of individuals who handle retirement plan data, and establish a procedure to train new employees when there is turnover or job attrition.
3. **Ask 401(k) service providers about their cybersecurity policies.** Reputable and established service providers (recordkeepers and TPAs) who offer retirement plan services to your company should have written information security measures that can be readily shared with clients. Before choosing to work with service providers, review their policies to ensure that they:
   - Have procedures for dealing with cybersecurity threats and the protection of your employee participants' personal information
   - Conduct risk assessments periodically to identify susceptibility to cybersecurity threats and the effect of potential business disruptions
   - Conduct an annual, independent assessment of their cybersecurity systems and policies
   - Employ a chief information security officer (or someone in an equivalent position)
   - Store, retain, and destroy sensitive data in a secure manner
   - Have a business continuity and disaster recovery plan that includes the recovery of your company's data after a breach

Remember to document the interaction and maintain the responses to add to your plan's fiduciary file.

According to a U.S. Small Business Association survey, 88 percent of small business owners felt their business was vulnerable to a cyberattack. Review your internal 401(k) information security controls and procedures to stay ahead of these criminals and the potential cybersecurity threats they pose. If you're unsure about where to start, talk to your retirement plan advisor or consultant.

## 401(k) Administration Basics: QDROs

When couples divorce, the resulting settlement often calls for the division of retirement plan assets. But how are these assets separated from a retirement plan participant's account? A qualified domestic relations order (QDRO) is a judgment, decree, or order for a retirement plan to pay child support, alimony, or marital property rights to a spouse, former spouse, child, or other dependents of a child (an alternate payee). Let's look at some key principles that every plan administrator should be aware of when handling a QDRO:

- Retirement plans must establish written procedures for administrating assets under QDROs. Be sure to locate and follow these procedures!

**401(k) Administration Basics: QDROs** *(continued)*

- Upon receipt of a QDRO, the plan administrator should notify the plan participant and the alternate payee(s) named in the order.
- The QDRO must specify the participant; the alternate payee; the last known mailing address of the participant and the alternate payee; the amount, percentage, or formula of the plan participant's benefits to be paid to the alternate payee (or payees); and the number of payments or time period to which the order applies.
- Former spouses who receive assets as the result of a QDRO distribution are responsible for paying the associated taxes. Taxes can be deferred by rolling the assets into an IRA or another qualified plan. **Please note:** QDRO distributions are not subject to the 10 percent early withdrawal penalty.
- A QDRO distribution that is paid to a child or other dependent is taxed to the participant.

Above all, it is imperative to adhere to the proper procedures when administering a QDRO. Failure to do so may result in significant operational failures. Plan administrators should lean on the expertise of their retirement plan service provider, TPA, or retirement plan advisor to guide them through the QDRO process.

## The Roth 401(k) on the Rise

The Roth 401(k) continues to gain steady adoption as a way for working Americans to defer in workplace retirement plans. According to Fidelity's Building Financial Futures report, the percentage of Fidelity's retirement plans offering a Roth 401(k) (which is contributed from an employee's salary on an after-tax basis) has increased by 32 percent in the past five years and is becoming increasingly popular with younger participants. Here are some additional insights from the report:

- The percentage of workplace retirement plans incorporating a Roth 401(k) deferral option into their plans offering is 75.2 percent, an all-time high.
- Millennials have increased their Roth 401(k) deferrals from 10 percent to 16 percent in the past 10 years, making them the generation to most take advantage of a Roth 401(k) option.
- In 2021, 26 percent of plans offer employees the ability to convert pretax assets to a Roth, twice the number who offered that option in 2016.

Does your company's retirement plan offer a Roth 401(k) option? If not, contact your retirement plan advisor to learn about how it can benefit your plan and employees.

## We Can Help

Contact us to learn more about 401(k) cybersecurity, QDROs, and the Roth 401(k). We're ready and willing to help.



Authored by the Retirement Consulting Services team at Commonwealth Financial Network.