How 401(k) Plan Sponsors Can Avoid The Scams And The Cons

By Ary Rosenbaum, Esq.

There is a saying I have about scams: "I'm from Brooklyn, you're going to have to get up earlier in the morning to get one on me." Growing up in Canarsie Brooklyn in the 1970s and 1980s allowed me to have street smarts, where I'm always looking behind my back. When someone is trying to do something that I think is suspicious, I always ask myself: "What's the con (confidence trick)?" In 26 years in the retirement plan business, I've seen a lot of scams and potential cons that I've seen (including exposing one or two). I know three people (a plan sponsor and two plan providers) who spent time in Federal prison for embezzling plan assets. The problem with scams and thefts is that while technology for 401(k) plans is improving, it's making it easier for thieves to steal. This is all about potential scams and avoiding getting scammed. You don't have to be from Brooklyn to understand how to avoid being scammed.

Make sure you have a reputable custodian.

When you set up your 401(k) plan, the money that your employees who are participants contribute must be held securely. It's the job of the plan custodian to safeguard the assets of the plan and the workers participating in it. The custodian's duties typically include: certifying balances of plan assets, and investing contributions to the plan as directed. The reason that Bernie Madoff lasted so long in conducting his Ponzi scheme was that he was the fund's advisor and he was the fund's custodian, so he could easily draft statements that assets were there, even if they weren't. Make sure that your plan has a reputable custodian. Any well-known mutual fund company, 401(k) platform, or insurance company will suffice. I can name you quite a handful out there, but I know I will offend someone if I don't mention their company's name, so I won't. You need a good, reputable firm that is well-known and financed. They will make sure the assets are, where they should be.

Make sure you have reputable plan providers.

I'm an attorney and you can easily check my status on New York's Attorney website and see my inactive status in Massachusetts and California. The same can be about a Certified Public Accountant to do your audit, their state licensing should appear on a state website. The same can't be said about a Third Party Administrator (TPA) because even my 19-year-old son could claim he's a 401(k) TPA since there isn't any state licensing or any other accreditation required. As a plan sponsor, you have a fiduciary duty to hire reputable plan providers. Jeff Richie owned a TPA in Texas called Vantage Benefits. He and his wife went to Federal prison for stealing $15 million from their 401(k) plan sponsor clients. A simple Google search before hiring Jeff and Vantage Benefits would have disclosed that he was sanctioned in 2008 by the Securities and Exchange Commission (SEC) and barred from the investment business for three years 'for conducting an unregistered and fraudulent offering' of securities in the retirement-services company he was running at the time." In Brooklyn, we call that a clue. I knew of a CPA who had two CPA firms, one that did regular accounting work for his clients and another firm, that allowed a TPA to conduct their plan audits. The Department of Labor (DOL) knew 3 employees (who were on the TPA's payroll) couldn't audit 80 plans. Anyone who wanted to know knew something would be up if the plan audit firm was in the same office as the TPA, while his "reputable" CPA firm was blocks away. The beauty of the Internet is information at your fingertips, you can simply vet any potential plan provider with a simple search. That goes for any plan provider, such as a TPA, advisory, attorney, and auditor. Always use common sense when you have a question about something that just doesn't seem right. As a 401(k) plan sponsor, you have a fiduciary duty and can't be an ostrich by burying your head in the sand.

Scams by participants

Twice, I dealt with plan participants who claimed someone else stole their distribution checks and cashed them. Of course, they wanted to be compensated for this theft. One was the fault of the bank. For the other one, we were provided camera footage from the check-cashing place involved. Yes, it was the plan participant cashing the check or an evil twin. All I know is that he accepted in writing that he did receive the distribution. Like people, most participants are going to be honest. Others just don't have that morality chip embedded in them and will try to score something they're not entitled to. I had to deal with a plan sponsor client with a former employee who conned their way into distributing their money into an IRA account managed by their outside broker while still working at the firm. I fixed that con by issuing a 1099R distribution form that caused the transaction to be a taxable event when he refused to return the money to the plan. You always have to be mindful of participants who see the 401(k) plan as a way to scam or some sort of revenge. That's why I advise plan sponsor clients to avoid having participants certify they qualify for a hardship. I just can't take people's word that they're undergoing some sort of financial hardship to get a distribution from their plan. Maybe because I'm from Brooklyn, I just don't take participants at their word. Also, you may have former employees who are aggrieved and want to take revenge on you for their termination. They may use a 401(k) plan that is inefficient and run terribly as hostage for a quick settlement on a lawsuit against you for a 401(k) plan. A retirement plan that is run correctly with good plan providers isn't likely to be the target of a former employee who wants to shake down their former employer for a quick settlement.

Being scammed by online thieves

A few weeks back, I got a random call from someone purporting to be from my crypto trading platform. This was coupled with texts that I didn't ask for, from the trading platform and Uber, with verification numbers because they claimed I asked for a password change. I didn't ask for a password change and it seems some of my passwords were leaked. I thought the phone call was odd since my crypto trading platform never calls, it's all done via email. Needless to say, something was off because he was insistent that he should shut down my account and that I should transfer my account to an online wallet. I knew this was a scam and he was aggravated that I claimed I didn't have a separate crypto wallet, so the scam failed. Again, common sense is needed to foil online thieves. When I started in this 401(k) business, every loan and distribution request was on paper. Thanks to technology, online requests for distributions and loans, make things easier. That also makes it easier for online thieves to hack and steal. A few years ago, a former employee in Estee Lauder's 401(k) plan settled with her former player and the plan's recordkeeper over $99,000 in authorized distributions made from her account. While we don't know the specifics of how these distributions were being made, similar situations have crept up where participants have had their assets stolen through impersonation. In many of these cases, there were red flags that the plan sponsor and/or TPA didn't identify. Cybersecurity is becoming an increased issue and the DOL is providing guidance to plan sponsors on this issue. It's incumbent on you to find out what cybersecurity policies your plan providers have in place. Make sure your plan providers are properly insured for cybersecurity issues. It's also important for you to identify any cybersecurity issues you may have, to avoid losses to participants within your 401(k) plan. You may want to consider evaluating your plan's cybersecurity issues, such as through a cybersecurity self-audit, adoption of a cybersecurity policy, or other improvements to the cybersecurity and/or monitoring processes.

The Rosenbaum Law Firm P.C.

The Rosenbaum Law Firm P.C.
734 Franklin Avenue, Suite 302
Garden City, New York 11530
(516) 594-1557
http://www.therosenbaumlawfirm.com
Follow us on Twitter @rosenbaumlaw