Cyber threats

Cybersecurity issues facing today's retirement plan sponsors

Fraud in the financial services industry has always been an issue. Early in my career as a lawyer, I was exposed to some very creative folks who went to great lengths for ill-gotten gains. Like many, I often asked myself what would have become of the fraudsters had they simply applied their skills to a more reputable line of work? Unfortunately, those devious minds are still at it.

The financial services industry has long been faced with the threat of someone making off with money that is not rightfully theirs. Crimes were often perpetrated by exploiting soft spots in institutional bureaucracies. In a paper world, forms were forged, accounts were bilked, fraudulent claims submitted and companies were exploited.

While the end goal of today's fraudsters has remained the same as their predecessors, they have at their fingertips what yesterday's fraudsters could only have imagined: the dark web; social media posts; online public records; and the ever-driving demand of clients for faster and faster delivery of services. Yesterday's would-be fraudsters generally had some specialized knowledge of the entities they targeted. Now that know-how is often gleaned from online sources and available in seconds to anyone with the time, diligence and interest to look.

It may be helpful to take a step back, hone in on some challenges facing our qualified plan industry (including what laws may apply) and think of some high-level action items. While depositary institutions and credit cards were some of the first targets of cyber fraud attacks, the qualified retirement plan industry is now being targeted. I don't think I've attended an industry conference in the past two years where significant time was not devoted to fraud. The good news is that our industry trade groups are quickly becoming educated on this topic and we are effectively sharing information. All of which is helping us to establish, improve and mature best practices and address vulnerabilities.

However, some headwinds exist. The first is the data that recordkeepers ingest. Qualified plan administration is often made more difficult by inaccurate, incomplete or nonexistent plan sponsor and participant data. The result of which can be detrimental to the services provided to the plan, where such services have data as a key building block. In the cyber context, the stakes can be much higher as accurate data is essential to knowing our customers and their plans. The more we know about our participants, the more accurately we are able to authenticate them. In turn, the better we are at preventing successful account takeovers.

DOL guidance

On the regulatory front, in April 2021 the Department of Labor (DOL) issued its first-ever guidance on the issue of cybersecurity. This has a two-fold effect - first, it is welcome news for plan sponsors and other fiduciaries as it provides some parameters upon which to base an analysis. However, it is also almost certain to usher in audit questions from the DOL surrounding cybersecurity.

The DOL guidance is divided into three parts: (a) Cybersecurity best practices; (b) Tips for hiring a service provider with strong cybersecurity practices; and (c) Online security tips.

The first two pieces of guidance are aimed at providing plans with information surrounding identification and mitigation of security risks, which includes analysis of third-party service providers. The final piece is aimed at individual participants and how they can help protect themselves.

One important overarching theme is process and documentation. It should come as no surprise that the DOL considers that "...responsible plan fiduciaries have an obligation to ensure mitigation of cybersecurity risks." Plan sponsors should review the guidance and consider how they can bring rigor, process and documentation in meeting their fiduciary obligations.

Considerations

Plan sponsors and fiduciaries are governed by prudent expert duties and the duties applicable to amounts being held in trust - respectively ERISA Sections 404 and 403. Procedural prudence in this context operates much the same as other fiduciary undertakings. Plan fiduciaries may wish to consider how they can demonstrate their diligence and document the process to both ensure the duty is met and, equally importantly, ensure they are comfortable with what procedures a recordkeeper might have in place.

Finally, vast amounts of personal information have been exposed through well-publicized data breaches.[1] I think that it's safe to assume that many people's general information (think date of birth, address, Social Security number) is floating out in cyberspace and available to bad actors. Knowing this, plan participants have a key part to play in helping to safeguard their own accounts. We should all be practicing good cyber hygiene! Here, some examples might include:

- Register your account with your financial institutions (qualified plans or otherwise)
- Activate available multi-factor authentication tools
- Review accounts frequently
- Use up-to-date anti-virus and electronic protection software
- Do not share log-in credentials
- Utilize strong and complex passwords or passphrases
- Educate yourself about online email scams
- Alert your financial institutions if your identity is stolen

Cybersecurity is a quickly evolving landscape for qualified plan recordkeepers, plan sponsors and participants. It is in everyone's best interest that all three constituents become educated on the risk and understand what steps might be taken to avoid successful fraud attempts.

Ted Schmelzle, JD, CIPP/US

Second Vice President, Customer Operations, Securian Financial

1. Swinhoe, Dan. "The 15 Biggest Data Breaches of the 21st Century." CSO, January 8, 2021.

securian FINANCIAL®

INSURANCE
INVESTMENTS
RETIREMENT

securian.com

400 Robert Street North, St. Paul, MN 55101-2098

F93689 Rev 7-2021 DOFU 7-2021
1701602