RETIREMENT PLAN CYBERSECURITY

Gallagher

Insurance | Risk Management | Consulting

There are no comprehensive federal regulations governing cybersecurity for retirement plans and their service providers.

Cybersecurity is a major concern in the context of retirement plans as plan participants' financial and personally identifiable information (PII)[1] is maintained and shared with multiple parties. If a cybercriminal has the appropriate information about a plan participant, they may be capable of taking an unauthorized distribution from an unprepared retirement plan. ERISA fiduciaries should be taking steps to protect themselves from potential liability.

From a national perspective, there are no comprehensive national laws, federal regulations or precedential cases governing cybersecurity, and no uniform framework for measuring the effectiveness of protections or governing cybersecurity for retirement plans and their service providers. Whether cybersecurity is an ERISA fiduciary responsibility and whether ERISA preempts state cybersecurity laws remain important unanswered questions. Recently, an official from the Department of Labor (DOL) said that the DOL was working on a guidance package addressing cybersecurity issues as they relate to retirement plan sponsors and service providers. He indicated this may include DOL investigations regarding the adequacy of various cybersecurity programs, especially for large plans, in terms of making sure the providers they hire are observing good cybersecurity practices.

With possible DOL guidance on plan sponsor and third-party vendor cybersecurity, as well as the increased participant awareness and sensitivity to the use, protection and disclosure of PII, many sponsors are taking actions to bolster their cybersecurity practices. The Society of Professional Asset Managers and Recordkeepers (SPARK) and the ERISA Advisory Council, among others, have made efforts in that direction.

CURRENT REGULATORY STRUCTURE:

The Safeguards Rule of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires that covered U.S. financial institutions safeguard sensitive data (15 U.S.C. 6801). Businesses that are significantly engaged in providing financial products or services, such as banks and brokers, are financial institutions that must safeguard customers' personal information. This personal information includes nonpublic information that is personally identifiable financial information (known as National Provider Identifier or NPI) collected by financial institutions. Information such as names, Social Security numbers, debt and payment history, and account numbers can be NPI when provided by the customer to the financial institution.

There is an understanding under DOL Regulation Section 2520.104b-1(c) and other pronouncements related to the electronic delivery of plan information that a plan sponsor must ensure the electronic system it uses keeps participants' personal information relating to their accounts and benefits confidential.

Both the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) have adopted a series of requirements for financial institutions servicing defined contribution plans. Financial service providers are required to develop and implement various security and confidentiality procedures and tools designed to detect fraud and theft. These requirements generally apply to a plan's consultants, investment advisers and service providers.

[1]PII is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g., Social Security number) that can identify a person uniquely, or quasi-identifiers (e.g., ZIP code) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

It may be difficult to argue that a prudent expert would not consider and react to cyber risks.

However, unlike the HIPAA rules (45 C.F.R. 160, 162 and 164) that apply to healthcare data for ERISA-covered healthcare plans, there is no clear ERISA regulatory structure governing the protection of financial information in retirement plans.

Some states have started to create their own laws, which typically address notifying participants of any breaches and private rights of action for any unauthorized disclosures of protected personal information. While several state attorneys general have been active in enforcing these laws in cyber breach cases, a state-by-state framework remains a patchwork solution.

FIDUCIARY PROTECTION:

ERISA imposes a standard of care on plan fiduciaries. One becomes a plan fiduciary either by being named as such, or through actions that result in the exercise of discretionary authority or control with respect to the management of plan assets; providing investment advice for compensation; or having discretionary authority or responsibility in the administration of a plan (ERISA § 3(21)).

ERISA fiduciaries are subject to the prudent expert standard of care and owe a duty of loyalty to the plan participants. A prudent expert acts with the care, skill and diligence that the circumstances call for a person of like character and like aims to use. Fiduciaries must discharge their duties solely in the interest of plan participants and beneficiaries for the exclusive purpose of providing benefits to those participants and beneficiaries (ERISA § 404).

Much consideration is given as to whether or not the responsibility to address cybersecurity is a fiduciary function. Assuming it is a fiduciary function, while the occurrence of a cybersecurity breach does not necessarily give rise to a fiduciary breach under ERISA, the failure to avoid, mitigate or respond to such a breach may create such exposure. This is because the rules of ERISA fiduciary liability are rooted in a duty to act with prudence. Due to the prolific nature of cyber attacks, it may be difficult to argue that a prudent expert would not consider and react to cyber risks. For this reason, retirement plan administrators and other fiduciaries should be cautioned against viewing protection of plan assets and participant information solely as part of the responsibility of external plan recordkeepers and third-party administrators (TPAs). Fiduciaries would be well served to demonstrate and document the development and implementation of their cyber risk management strategies and due diligence.

Although ERISA's preemption of state laws is well established, the extent to which ERISA preempts state privacy and data laws is currently being litigated. Accordingly, retirement plan sponsors and administrators should not disregard state laws in developing and implementing their cyber risk management strategies.

POTENTIAL FIDUCIARY LIABILITY—A RISING ISSUE?

After almost three years of litigation in the excessive fee case involving Vanderbilt University's two 403(b) retirement plans, the parties announced a settlement agreement. One aspect of the settlement had an interesting turn: Vanderbilt must take additional steps to protect confidential participant information.

In addition to excessive fee violations, the plaintiffs in the Vanderbilt case claimed the committee breached its duties of prudence and loyalty, and participated in prohibited transactions by allowing TIAA to misuse confidential participant information for its own benefit.

The plaintiffs argued this information was a plan asset, and the committee did nothing to stop TIAA from using the information to sell participants its investment products and wealth management services outside of the plan.

The settlement requires Vanderbilt to contractually prohibit the recordkeeper from using information about participants acquired throughout the course of providing services to the plan to market or sell unrelated products or services to the participants, unless a request for such products or services is initiated.

While the settlement does not serve as legal precedent, it could be viewed as acknowledgment of the value of participant data. In fact, in a 2020 settlement of ERISA fiduciary breach claims, Oracle Corporation agreed that, for a period of three years, they will instruct the plan's recordkeeper in writing that it must not solicit current plan participants for the purpose of cross-selling non-plan products and services. It is quite possible that similar claims constructed around the value of plan and participant information could surface in future complaints.

More recently, a retirement plan participant in the Abbott Laboratories plan filed a fiduciary breach suit against Abbott Labs and its plan recordkeeper, Alight Solutions. According to the plaintiff's claim, a cyberthief used the "forgot my password" feature on the plan's online recordkeeping platform to access her account. The thief ended up taking a large unauthorized distribution from the account. The participant's suit made a claim for approximately $245,000 in benefits, plus earnings and fees.

The plan's recordkeeper was audited by the DOL and has been subjected to prior suits relating to security issues, which could serve as the basis for the argument that Abbott Labs did not act as prudently as they should have in selecting their service providers. The lesson for plan sponsors is that failing to focus carefully on cybersecurity risks can result in very specific (and potentially expensive) liabilities.

This case underscores the urgency in enacting and complying with prudent procedures to protect the electronic security of participant accounts, especially during a time where participant withdrawal requests are on the rise. Further complicating matters, the current economic climate is new and unprecedented. First, the COVID-19 pandemic crisis has led to increasing unemployment and furloughs. With a loss in steady income, participants are turning to their retirement plans for cash. Second, the Coronavirus Aid, Relief, and Economic Security (CARES) Act legislation made it easier for participants to withdraw money from their retirement accounts and reduced the chance of tax penalties, which only made plan withdrawals more popular. Finally, more employees working remotely, and possibly on unsecure networks, creates another challenge for plan sponsors in protecting confidential data.

89% of employers do not know if their employees' and/or executives' home networks are secure, or not part of command and control/botnet.

Source: Gallagher 2021 Cyber Insight Report—of 517 respondents.

One of the best protections is thorough training for both HR staff and employees.

The process of assessing security is further complicated by a destructive information cycle.

of employers felt informed about their fiduciary responsibilities and potential liability when it comes to cybersecurity and protecting plan participant data.

Source: Gallagher's 2020 Retirement Pulse Survey

Given the focus on the value of personal data in our society, a conservative approach is to treat plan participant financial data as being a plan asset and take prudent steps to protect it as such. We expect that ownership and control of participant data will continue to be an area of intense interest in the retirement industry, and could well be the subject of future court decisions.

PLAN SPONSORS SHOULD TAKE A PRUDENT APPROACH.

For HR leaders, making prevention the first imperative requires working with corporate IT to put safeguards in place. They should have clear sight into how and where data is collected, held and classified; who has access; and which laws apply. Investing in enterprisewide technology is critical to recognizing cyber attacks and stopping them when they occur. Implementing and periodically testing a disaster recovery plan that includes employee benefits leaves the response team well prepared. In its comments about possible DOL guidance on cybersecurity, the DOL mentioned that the response time to an incident would be a consideration in the guidance, as well as investigations.

In many cases, the greatest vulnerability to cybertheft is the HR team itself. Phishing and other social engineering techniques have become very sophisticated and can easily fool unwary team members into divulging information that gives thieves access to sensitive data. One of the best protections is thorough training for both HR staff and employees.

ERISA does not mandate a written cybersecurity or financial information policy, and there is no one-size-fits-all approach that must be taken. Instead, a plan sponsor must act prudently. The easiest way to show that a plan sponsor has followed a prudent process is to document that process. Creating any prescriptive document beyond those required by ERISA can carry significant challenges and risks, so cybersecurity documents should focus on process items rather than attempting to lay out any hard and fast rules.

Additionally, ERISA's duty to monitor the plan's service providers also implies that fiduciaries should inquire about the security measures being implemented by the plan's recordkeeper, trustee and other providers. The process of assessing security is further complicated by a destructive information cycle. Recordkeepers have significant incentives to reveal only a limited amount of information about their cyber defenses because hackers can learn from extensive revelations and adapt their methods to avoid detection. This means that recordkeepers often rationally respond with only limited information about cyber attacks and security.

Cyberthreats for retirement plans are unique. Retirement plans should not simply work from a generic cybersecurity checklist that does not address the specific challenges they face.

76% of organizations are not aware of all data protection requirements remote workers must comply with.

Source: Gallagher 2021 U.S. Cyber Insights Report

PLAN SPONSORS SHOULD CONSIDER:

- A process for addressing and fixing cybersecurity issues; for example, identify possible gaps in security in the information-sharing process with TPAs and recordkeepers.
- Ensure that the appropriate level of cyber liability insurance is in place (for both the employer and vendors) to help mitigate the damage of any potential attack, and be sure that such coverage is as broad as possible.
- Document the process for moving plan data, maintain a data inventory, retain only data needed and, if data elements can be redacted, do so.
- Maintain an internal inventory of where information is stored within the company, and also which third parties it is transferred to, and appropriately restrict.
- Implement processes and controls to restrict access to plan systems, etc., and possibly create routine reviews of access controls to files, information, and vendor access and authority to direct third parties.
- Delete records that are no longer necessary, and make sure providers do the same.
- Consider retaining an outside firm that specializes in cybersecurity for retirement plans to ensure that participants' data is secure through periodic audits.
- Thoroughly vet service providers, and negotiate contract provisions to lower or mitigate the cost of correcting a possible cyber attack on a plan by allocating responsibility to the vendor. Add questions about data security to any RFP process.
- Request a copy of a provider's report on controls SOC-II, an audit report describing an organization's internal controls and attesting to their strength.
- Perform a fiduciary review of their providers' SOC reports, and make sure that the reliance the recordkeeper is placing on the client for their part is understood and in place.
- Implement processes and controls to restrict access to plan systems, applications, data and other sensitive information. Share any plan-related information strictly on a need-to-know basis.
- Consider revising service agreements to require notification when breaches occur, and indemnification and/or sanctions for any losses resulting from a breach.
- Develop a retirement plan-specific cybersecurity risk management strategy—in short, have a plan in place to address your response to a breach (including appropriate participant notices and other remediation efforts in the event of a breach).
- Consider requiring two-factor authentication to access participant accounts.
- Limit the transmission of PII by using other forms of non-recognizable identification (such as employee number).
- Establish necessary policies and training on user authentication and password procedures.

CYBER AND FIDUCIARY INSURANCE

How confident is the organization that cyber incidents involving its remote workforce would be covered by its insurance?

Source: Gallagher 2021 U.S. Cyber Insights Report

PLAN SPONSORS SHOULD ENCOURAGE PLAN PARTICIPANTS TO:

- Set up an online account. Without an online account, the participant's vulnerability to fraud is greatly increased, because it allows hackers to set up new online accounts and gain access to a participant's funds.
- Choose strong passwords that are hard to guess and change them frequently.
- Store passwords with care — do not leave passwords on a desk, table or counter for others to see.
- Log out completely when leaving any plan-related web or intranet site.
- Be aware of social engineering risks, methods and defenses, and the heightened risk that will unfortunately arise from COVID-19-related scams.
- Never provide login credentials in response to an email request.

The cybersecurity environment for retirement plans is undergoing significant evolution, and this evolution will accelerate.

Fiduciary insurance is typically triggered when a lawsuit is filed or regulatory investigation has commenced (or sometimes when a regulator asserts a deficiency), while cyber insurance is often triggered by a data breach. Existing fiduciary insurance may help after a lawsuit is filed, but prior to that point, the plan and/or plan sponsor may be responsible for the costs and mechanics associated with a breach (depending on the terms of the insurance policy).

Plan sponsors may wish to seek specific cyber insurance policies or riders to existing policies (some of which are available in the market today) to cover their employee benefit plan(s). Policies that provide benefits after a breach can offer assistance in locating the appropriate personnel to address each step of the process, from determining the scope of the breach to notifying the appropriate individuals or entities, to providing resources to mitigate or make whole any damages suffered as a result of the breach, such as identity monitoring or replacing stolen assets.

CONCLUSION:

The cybersecurity environment for retirement plans is undergoing significant evolution, and this evolution will accelerate. While the precise fiduciary obligations of plan sponsors with respect to plan and participant information are not yet clearly defined, it is clear that multiple efforts are underway to define those obligations and respond to the increasing need to strengthen protections. Presently, the SEC, the DOL, multiple states, and key industry organizations like SPARK and the ERISA Advisory Council are working to regulate cybersecurity for retirement plans and develop increased protections.

Sources:

Industry Best Practice Data Security Reporting. The SPARK Institute, Inc.
DOL to Issue Guidance, Ramp up Investigations on Cybersecurity. NAPA-net.org.
Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective. Pension Research Council.
Securing a successful HR and benefits technology strategy. Arthur J. Gallagher & Co. Human Capital Insights Report.
Vanderbilt 403(b) excessive fee case settlement goes beyond monetary relief. Arthur J. Gallagher & Co. Retirement Plan Consulting Practice whitepaper.
Bartnett v. Abbott Laboratories et al., No. 2020 CV 2127, (N.D. Ill. filed April 3, 2020)
Cyber Security and Retirement Plans. Retirement Learning Center.

GBS39674

ajg.com