Cybersecurity Creates Ongoing Challenges for Plan Fiduciaries and Recordkeepers

Carol Buckmann[*]

Cybersecurity threats to retirement plans are increasing, and plan fiduciaries and recordkeepers must take steps to prevent imposters from stealing plan benefits and to keep plan data secure. They need to be aware of Department of Labor Best Practices, current litigation, and available general resources on establishing good cybersecurity procedures.

WHO IS LIABLE IF A HACKER STEALS A PLAN PARTICIPANT'S BENEFITS?

Internet thieves haven't spared retirement plans, but the surprising answer is that we still don't know. There is no federal law providing automatic recovery in these situations, and no legal requirement that those who handle distributions maintain cybersecurity insurance or indemnify participants if their negligence allows a thief to steal the participant's retirement benefits. Despite this lack of clear binding guidance and remedies, plan fiduciaries and recordkeepers must take steps to prevent imposters from stealing plan benefits and to keep plan data secure. They need to be aware of litigation in this area and utilize available resources.

Why Is ERISA Responsibility Unclear?

While maintaining the security of plan data and assets is a fiduciary responsibility, at least in the 401(k) and defined benefit space, where plans are not subject to HIPAA's privacy and security requirements, there are no binding rules setting out what fiduciaries must do. The Department of Labor has issued helpful best practices and recommendations for fiduciaries and recordkeepers, which clearly state that "[r]esponsible plan fiduciaries have an obligation to insure proper mitigation of cybersecurity risks,"[1] but these practices are recommended, not mandatory. To further complicate the problem, recordkeepers whose systems have been breached are not generally considered fiduciaries for purposes of ERISA, as they don't assume discretion over plan administration or investments.[2] Service provid-

[*]*CAROL BUCKMANN* is a co-founding partner of Cohen & Buckmann P.C. With a career that spans more than 40 years, Carol has become one of the foremost employee benefits and ERISA attorneys in the country. She is widely known for her in-depth understanding of issues related to ERISA, including pension plan compliance, fiduciary responsibilities and investment fund formation. She writes for the firm's blog, Insights, and has contributed articles and practice notes to many industry publications. In addition to opining about new developments in the benefits industry, Carol also speaks frequently at industry and client events. She has been recognized by Super Lawyers, Best Lawyers, Chambers USA and Martindale.

ers that are not fiduciaries do not have a duty under ERISA to safeguard plan data and assets. Although ERISA requires that those who handle plan funds must be bonded against losses due to their fraud or dishonestly,[3] ERISA bonds do not cover losses due to the fraud or criminal behavior of unrelated third parties.

Other Legal Protections

There are some specific laws besides ERISA that might provide requirements or a basis to sue in the event an account is stolen or data security is breached. For example, financial institutions are required by the Gramm-Leach-Blilely Act[4] to establish rules to protect the privacy of consumer financial information. State laws such as California's may also impose data protection and privacy requirements, and state negligence law might provide a recovery if a recordkeeper's inadequate protections allowed an account to be stolen. However, this is a patchwork of protections that may vary depending on where the participant or other parties are located. There is no uniform national law that applies to everyone across the country.

For all of these reasons, plan participants are vulnerable to losing their entire retirement savings when a security breach occurs. Not surprisingly, 401(k) participants whose accounts were stolen and who were not made whole by their recordkeeper or plan sponsor have gone to court seeking to have their accounts restored, but no clear legal standards have been developed in this litigation to date.

WHAT ARE THE KEY ISSUES?

In the ERISA lawsuits, plan sponsors, plan committees, recordkeepers and even custodial trustees have been sued, but they have different roles and responsibilities. In the absence of black and white rules, courts are required to make a determination of whether the party responsible for any breach is a fiduciary and, if so, whether a fiduciary breached ERISA fiduciary responsibilities in failing to have appropriate protections in place. If defendents include the plan sponsor or a plan committee, a court could look at whether they adequately investigated and monitored their vendors' cybersecurity systems both when the vendors were hired and on an ongoing basis.

Since no procedures are guaranteed to prevent cybersecurity breaches, a court might determine that the fiduciaries who have addressed cybersecurity issues have not breached their responsibilities and that the plan's recordkeeper, even if not a fiduciary, had reasonable cybersecurity procedures. In that case, an innocent participant whose benefits were stolen would not be entitled to reimbursement.

There may also be claims under a recordkeeper's service agreement with the plan, which provide for indemnification of losses due to gross negligence or willful misconduct of the recordkeeper's employees and may also establish minimum performance standards. The participant will not be a direct party to these contracts, but the plan's fiduciaries can assert them.

One ERISA and Internal Revenue Code claim that has not been raised so far in the litigation is whether failure to restore a stolen account improperly deprives the victim of a vested benefit.[5]

THE REPORTED CASES

Initially, it appeared that vendors were quietly reimbursing participants whose accounts were lost due to cyberfraud, but lawsuits began to be filed in cases where this did not happen.

Estee Lauder

The first important case involved a participant in the Estee Lauder plan and the re-

cordkeeper Alight.[6] The participant lost $99,000 and alleged that Alight had inferior cybersecurity protections. An Alight employee actually assisted the thief to change passwords and steal the account. The thief requested that three separate distributions be sent to three separate banks, which the participant argued should have raised red flags. This case was settled before the court could deal with the legal responsibilities involved.

Abbott Laboratories

This case[7] also involved a breach allegedly facilitated by recordkeeper employees. A call center employee helped to facilitate the breach by sending the thief a one-time code to change the password and giving the participant's address to the thief. The plaintiff whose account was stolen sued Abbott and its committee as well as the recordkeeper. The participant claimed that Alight was a fiduciary because it controlled plan assets and had violated the duties of prudence and loyalty. Since Alight had been involved in previous breaches, Abbott should not have hired Alight. A pre-trial decision dropped Abbott defendants from the case, stating that there was no showing that actions taken by Abbott were objectively unreasonable, but left Alight as a defendant.

The Disberry Case

One of the most publicized cases involved the theft of Paula Disberry's 401(k) account valued at around $750,000 from a 401(k) plan maintained by Colgate-Palmolive.[8] Again, recordkeeper (Alight) employees assisted the cyber criminal to change the account's password and address, enabling the criminal to steal her account. Although Disberry lived outside the United States, a confirmation of the transaction was sent to her by snail mail, which was intercepted by the thief.

Disberry didn't find out about the theft until after her account had been emptied. She then filed for restoration of her account under the plan's claims and appeals procedure, and was reportedly told by the committee that the plan had paid out everything she was owed. Not surprisingly after such a response, Disberry sued the plan committee, Alight, and its custodial trustee Bank of New York/Mellon for breach of fiduciary duty in allowing the breach to occur. The complaint alleges that an Alight employee assisted the thief to change a password, the mailing address for the participant and bank information for the distribution without notifying the participant in real time or requesting immediate confirmation of the transaction.

It is interesting to note that the thief also tried to steal Disberry's pension from a Colgate-Palmolive defined benefit plan, but was thwarted by a different recordkeeper's insistence on seeing photo ID, which the thief could not produce. Sometimes simple precautions, not high tech defenses, can prevent benefit theft.

In a preliminary decision, Disberry's claims against the Bank of New York were dismissed, as monitoring distributions was not part of its responsibilities as directed trustee. The court refused to dismiss the fiduciary breach claims against the committee or Alight, and took the unusual step of suggesting that plaintiff should add an alternative state law negligence claim against Alight to the complaint.

The *Disberry* case has the potential to establish new law in this area, and benefits professionals should be on the alert to see if there are further developments.

MandMarblestone Group

This case[9] involving a stolen 401(k) account is notable because the thief apparently gained access to documents allowing them to claim benefits

by hacking into the home computer of a participant who was working remotely, then posed as the office administrator and directed that distributions of $400,000 be made from the account of the plan trustee, who was also a principal of the plan sponsor and listed as administrator in plan documents. The participant sued Nationwide as custodian of the funds as well as third party administrator Mand-Marblestone Group. Nationwide argued in its defense the "There is no fiduciary duty to prevent forgeries." Nationwide also counterclaimed against the plaintiffs, claiming that their negligence contributed to the breach, as they were aware of unusual account activity.

In the end, the court, which seemed to be looking for a rationale to protect the participant, found that the recordkeeper and custodian were fiduciaries, though this is inconsistent with other cases on these issues. The court also ruled that it would not take into account the plaintiff's activities in reviewing the obligations of the fiduciaries, since fiduciaries may not reduce their own liability by alleging that other parties were negligent. However, Nationwide might later seek indemnification from the plaintiff. This case is a warning to company fiduciaries that their own cybersecurity practices and standard of care will be reviewed if they seek recovery of stolen benefits from their third party vendors.

SERVICE PROVIDER WARRANTIES

As a result of publicized account theft, and these earlier cases, several major 401(k) vendors have provided cybersecurity warranties to their plans. Subject to conditions that plan fiduciaries should review with their ERISA counsel, these warranties will reimburse participants whose accounts were stolen from the recordkeeper's system through no fault of their own.

DATA BREACH CASES

Plan data is also considered valuable, and another reason good cybersecurity practices are needed is that cyberthieves may use stolen personal data to apply for other benefits, credit cards, or loans in the participant's name. In that case, issues arise as to how quickly participants are notified of the breach and what remediation will be provided. The typical relief offered is for the party incurring the breach to pay for credit monitoring of affected participants for a limited period of time. However, this may not be sufficient, as it may be years before stolen data is used.

MOVEit Data Breach

Recently, a breach involving PBI and MOVEit exposed participants in CALPERs and Tennessee state retirement plans and customers of TIAA (and many other entities) to fraud by criminals using their personal information. Two class actions have been filed by CALPERs participants as a result of the breach.[10] The plaintiffs claim that they were notified too late and that limited credit monitoring is an insufficient remedy. They seek to bar CALPERs from using these vendors going forward among other relief. The state plans are not subject to ERISA, but plaintiffs in the CALPERS cases set forth several claims under California state law. They did not name CALPERS as a defendant. TIAA has also been sued as a result of this breach[11], including for violating the Gramm-Leach-Bliley Act. One of the complications in these lawsuits is that the breach occurred at a company retained by the contracting party.

These cases may develop law regarding breach notification obligations or the remedies to which participants whose data has been stolen are entitled.

In the future, participants may be assisted in coping with the consequences of a data breach by a new SEC rule[12]

that requires public companies to disclose material breaches within four business days. State consumer and privacy laws also may provide causes of action for participant victims in addition to any remedies provided under ERISA.

WHAT ARE PLAN FIDUCIARIES TO DO?

Even in the absence of clear and uniform legal rules, all plan fiduciaries need to take steps to protect their participants from cybertheft and data breaches, particularly since the Department of Labor can be expected to ask questions about plan cybersecurity as part of any audit. There are many practical steps they can take.

DEPARTMENT OF LABOR BEST PRACTICES

The Department of Labor has not sued plan sponsors or recordkeepers for failing to prevent breaches, although it initiated an investigation of recordkeeper Alight, the defendant in lawsuits mentioned above. There are no regulations or advisory opinions fleshing out these legal obligations. However, the Department has issued a document setting out best practices for plan recordkeepers[13] and a second containing "Tips for Hiring a Service Provider with Strong Cybersecurity Practices."[14] These should be must reading for plan sponsors and recordkeepers.

Recordkeeper Best Practices

The Department of Labor best practice recommendations for recordkeepers include the following:

- Have a program in place to deal with security incidents and disaster recovery
- Conduct prudent annual risk assessments
- Have annual third party audits of security controls
- Have assigned employee roles
- Encrypt sensitive data, including in transit
- Conduct regular employee training
- Document the framework used to assess its system and practices
- Review access privileges every three months
- Confirm the identity of the authorized recipient of funds
- Trigger an alert when account information is changed, and require additional validation if personal information is changed prior to a request for distribution
- In case of a breach, notify law enforcement, the appropriate insurer, and particpants, giving participants the information necessary to protect themselves from unauthorized use of their data.

In the case of an audit, be able to produce audit reports, audit files, penetration test reports and supporting documents.

Tips for Plan Sponsors

Plan sponsors have ongoing obligations not limited to hiring. The following are recommended for hiring and during the term of the service relationship:

- Ask about policies, procedures and audit results, and compare them to industry standards, looking specifically for outside auditors and insurance coverage.
- Review public information about breaches and litigation
- The service agreement should:
    1. Require compliance with all applicable laws
    2. Prevent unauthorized

use and disclosure of data

3. Deal with breach notification
4. Allow the plan sponsor to monitor whether the recordkeeper is complying with the agreement's requirements on an ongoing basis
5. May require maintaining cybersecurity insurance coverage
6. Given the practice of vendors to outsource responsibilities to subcontractors, who may be outside the United States, an often overlooked issue is that the agreement should require the vendor to ensure that any subcontractors it hires will satisfy the same cybersecurity standards as apply to the vendor and its employees, and its indemnification provisions should make the vendor responsible for actions taken by its subcontractors as if they were the vendor's own employees.

In addition, it is important for plan sponsors to understand that their own data systems should satisfy the requirements recommended for recordkeepers, including employee training and third party systems audits. As more and more employees work remotely, the *MandMarblestone* litigation makes clear that it is also essential to control security on laptops and home devices.

OTHER SOURCES OF INFORMATION

There are many other resources available to plan sponsors who want to develop strong internal technology and procedures but may not have or have limited internal cybersecurity expertise. The Society of Professional Asset Managers and Recordkeepers (SPARK) Institute releases reports on best practices for the retirement industry. Much helpful general information on establishing good cybersecurity practices is also available from the federal government. Plan sponsors should be familiar with the National Institute of Standards & Technology (NIST, part of the U.S. Chamber of Commerce), and its framework of best practices. The federal Cybersecurity & Infrastructure Security Agency (CISA) is another source of helpful information and best practices. Plan sponsors looking for providers to review their systems can also hire outside vendors who will guide them through an RFP to find the right person to hire.

A BETTER PATH GOING FORWARD

There is more regulation of data breaches and responses to them than clear protection against outright benefit theft. Benefit theft is a crime, but criminal authorities cannot be counted upon to recover stolen benefits. The fact that some participants whose benefits were stolen by thieves had no practical recourse except suing all parties involved in a breach is troubling given the importance of retirement security and the need to increase Americans' retirement savings.

Reliance on state law to solve this problem defeats ERISA's purpose of having uniform rules apply to pension benefits. There is a need for a federal solution to these problems, either via new regulations or new laws. If we are concerned that participants aren't currently saving enough for retirement, forcing them to go to court to try to recover stolen benefits won't help and may even deter some employees from participating in their plans.

Here are some suggestions to help control the problem of stolen benefits:

- Requiring recordkeepers and plan sponsors to maintain cybersecurity insurance of at least a minimum overage level
- Binding regulations requiring third party systems audits and employee cybersecurity training
- Requiring all recordkeepers to provide cybersecurity warranties
- Establishing a federal program to reimburse participants whose benefits are stolen through no fault of their own.
- Binding authority from the DOL on the liability of plan fiduciaries for these thefts
- Development of sample service agreement provisions by the DOL to assist those negotiating service agreements. This will be especially helpful to smaller plan sponsors without regular outside ERISA counsel.

Some of these changes would require Congressional action, but they would reinforce the importance of protecting plan participants from losing their retirement savings through no fault of their own.

NOTES:

[1]See dol.gov/files/ebsa/key-topics/retirement-benefits/cybersecurity.

[2]ERISA Section 3(21), 29 U.S. Code 1002(3)(21).

[3]ERISA Section 412, 29 U.S. Code 412.

[4]15 U.S. Code 6809.

[5]See 26 U.S. Code 411(d).

[6]Bilello v. Estee Lauder, 1:20 cv-o4770 (S.D.N.Y, motions to dismiss denied June 7, 2021 and July 26, 2021), complaint available at 2020 WL 10817328.

[7]Bartnett v. Abbott Laboratories, 492 F. Supp. 3d 787, 2020 Employee Benefits Cas. (BNA) 380295 (N.D. Ill. 2020).

[8]Disberry v. Employee Relations Committee of Colgate-Palmolive Company, 2022 WL 17807122 (S.D. N.Y. 2022).

[9]Leventhal v. MandMarblestone Group LLC, 2020 Employee Benefits Cas. (BNA) 197040, 2020 WL 2745740 (E.D. Pa. 2020).

[10]The first of these was Berry v. Pension Benefit Information LLC, 4:23-cv-03297 (N. D. Cal., filed June 30, 2023).

[11]Jentz v. Teachers Insurance and Annuity Association of America, 1:23-cv-06944 (S.D.N.Y., filed August 7, 2023.

[12]88 Fed. Reg. 51896, August 4, 2023. This final rule is effective September 5, 2023.

[13]Cybersecurity Program Best Practices, dol.gov/files/ebsa/key-topics/retirement-benefits/cybersecurity.

[14] Dol.gov/files/ebsa/key-topics/retirement-benefits/cybersecurity.tips-for-hiring-a-service-provider-with-strong-security practices.