ERISA Fiduciary Concerns Relating to Cybersecurity: Theft of Plan Assets

A Practical Guidance® Article by José M. Jara, Fox Rothschild LLP

José M. Jara
Fox Rothschild LLP

The 1920s and 1930s were infamous for bank robberies, where robbers disguised themselves as Santa Claus and answered questions by stating that banks are robbed "because that's where the monies at." Texas State Historical Association (6/1/96); FBI, Willie Sutton; see also Helms v. State, 112 Tex. Crim. 203, 205 (Tex. Crim. App. 1929). Fast forward about 100 years, cybercriminals do not need to disguise themselves as Santa Claus, and as to where the "monies at" – well, U.S. retirement plan assets totaled $36.7 trillion as of the second quarter of the 2023. See U.S. Library of Congress. Congressional Research Service. U.S. Retirement Assets: Data in Brief, Office of Congressional Information and Publishing, (9/20/23). Since a cyber breach is not a matter of if it will occur, but a matter of when, fiduciaries of retirement plans should be addressing this risk. This blog will discuss the U.S. Department of Labor (DOL) authority over cybercrimes, litigation involving cyber theft of participants' accounts, and risk mitigation techniques for plan fiduciaries.

ERISA 101

The Employee Retirement Income Security Act of 1974 (ERISA) is the statute that regulates retirement plans. Companies that sponsor retirement plans must have named fiduciaries (or appointed fiduciaries), who are persons with the discretionary authority or control over the administration or investment of a plan. Persons not named or delegated to be fiduciaries but who have this discretion may be deemed *de facto* fiduciaries because of their actions. Fiduciaries must carry out their obligations for the "exclusive purpose" of the plan's participants and beneficiaries (duty of loyalty) and with the "care, skill, prudence and diligence under the circumstances then prevailing that a prudent [person] acting in like capacity and familiar with such matters would use in the conduct of an enterprise of like character with like aims" (duty of prudence). ERISA § 404(a)(1)(A), (B) (29 U.S.C. § 1104(a)(1)(A), (B)).

Moreover, fiduciaries are prohibited from engaging in certain transactions, unless an exemption applies. One prohibition includes a fiduciary not to engage a service provider for the furnishing of services to the plan. ERISA § 406(a)(1)(C) (29 U.S.C. § 1106(a)(1)(C)).

The exemption to contract with a service provider requires that: the services are necessary for the operation of the plan, the contract with the service provider is for reasonable fees, and the contract itself is reasonable as a whole. ERISA § 408(b)(2) (29 U.S.C. § 1108(b)(2)). Other prohibited transactions include the fiduciaries' avoiding conflicts of interest or self-dealing. ERISA § 406(b) (29 U.S.C. § 1106(b)).

U.S. Department of Labor

The DOL has expressed grave concerns about this topic. Back in 2016, the ERISA Advisory Council issued a report recommending that the DOL publish on its website materials for plan sponsors and fiduciaries to utilize when developing a cybersecurity strategy and program. Yet, to date, no official regulations have been published by the DOL, leaving plan fiduciaries not in the "dark web" but in the dark.

Nonetheless the DOL has posted on its website three brochures to assist fiduciaries in meeting their responsibilities as they relate to cybersecurity.

- Tips for Hiring a Service Provider: provides certain questions plan sponsors should ask when selecting a service provider to determine if they have strong cybersecurity practices. One of them includes what type of insurance policies does the service provider have to cover losses caused by cybersecurity and identity theft breaches. The DOL also highlights the point that fiduciaries need to make sure that the service provider contract include ongoing compliance with cybersecurity and information security standards.
- Cybersecurity Program Best Practices: assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks. The DOL here spells out in greater detail what a service provider should have such as: a formal well documented cybersecurity program, annual risk assessments, reliable annual third-party audits of security controls, and periodic cybersecurity awareness training.
- Online Security Tips: aids plan participants and beneficiaries who check their retirement accounts online to reduce the risk of fraud and loss. The DOL highlights the use of strong and unique passwords, use of multi-factor authentication, and awareness of phishing attacks.

While the brochures are considered only guidance, the DOL in its investigations have inquired into whether any of this guidance was implemented. In particular, they question whether their guidance has been followed in regard to hiring a service provider.

If there's any doubt as to the DOL's jurisdiction over cybersecurity, the 7th Circuit has erased some of that doubt by finding that the DOL has broad investigative authority to investigate whether cyber breaches resulted in ERISA violations. The DOL, through its subagency the Employee Benefits Security Administration, has investigative authority to determine whether any person has violated Title I of ERISA (the reporting and disclosure, fiduciary responsibility, vesting, minimum participation and funding provisions) or any related regulations or orders. ERISA Section 504, 29 U.S.C. 1134. Relying on ERISA's duty of loyalty and duty of prudence, the 7th Circuit stated: "[t]he reasonableness of [service provider's] cybersecurity services, and the extent of any breaches, is … relevant to determining whether ERISA has been violated—either by [the service provider] itself, or by the employers that outsourced management of their ERISA plans to [the service provider]. Walsh v. Alight Sols. LLC, 44 F.4th 716, 723 (7th Cir. 2022).

Thus, even without regulations in place, fiduciaries should embrace cybersecurity as an issue they need to address under the duty of loyalty and duty of prudence. For starters, it would entail reviewing DOL's guidance, and when contracting with its service providers asking the questions laid out by the DOL. Other potential risk mitigating techniques involve addressing cybersecurity in the service contract itself and possibly the duty for continuously upgrading cyber protocols.

Litigation

On the litigation front, a recent lawsuit highlights the cybercrime threat. In Disberry v. Emp. Rels. Comm. of Colgate-Palmolive Co., 646 F. Supp. 3d 531 (S.D.N.Y. 2022), the participant lives in South Africa and had an account worth $750,000 in the Colgate-Palmolive 401(k) plan. The fraudster called the plan's benefit hotline to update the participant's contact information, intercepted various passcodes, and changed the participant's address to Las Vegas, Nevada. The fraudster subsequently requested a distribution and wiped out the participant's entire account. The participant filed a lawsuit since the participant wasn't being reimbursed by the plan sponsor, recordkeeper, or custodian.

On a motion to dismiss, the court ruled as follows:

- **Fiduciaries – motion to dismiss was denied.** The Court did find that the participant's ERISA breach of fiduciary duty complaint was "thin" but was reluctant to dismiss the case against the fiduciaries. However, notably the court acknowledged that fiduciaries need only reasonable procedures in place, but not air-tight procedures to protect against heinous crimes like the one in this case.
- **Service Provider – motion to dismiss denied.** The Court found the following allegations were plausible: that the service provider was a de facto fiduciary, was the only party interacting with the fraudster, and should have seen the red flags.
- **Custodian – motion to dismiss granted.** The Court found the custodian had no discretion or control since it was a directed trustee.

This case is instructive and based on the facts of this case, an ERISA breach of fiduciary can pass the motion to dismiss stage as against the plan's fiduciary and service provider for a cybercrime.

In Leventhal v. MandMarblestone Grp. LLC, No. 18-CV-2727, 2019 WL 1953247, at *1 (E.D. Pa. May 2, 2019) a participant's account was also wiped out by a cybercriminal to the tune of $400,000. The cybercriminal was able to obtain a former legitimate withdrawal request, used this information, and requested withdrawals to be directed to a new bank account. This is another case where the ERISA breach of fiduciary claim survived a motion to dismiss, this time against a third-party administrator and custodian. However, note that the participant's claims for breach of contract and negligence were dismissed. The state law claims were dismissed as

ERISA preemption provisions provide that: "ERISA 'shall supersede any and all State laws insofar as they relate to any employee benefit plan' covered by the statute." Leventhal v. MandMarblestone Grp. LLC, No. 18-CV-2727, 2019 WL 1953247, at *7 (E.D. Pa. May 2, 2019).

What is also important about this case is that while the court found the 3rd Circuit has not ruled on this issue, it held that under traditional trust law the service provider could maintain a counterclaim against a fiduciary under ERISA for contribution and indemnity. See Leventhal v. MandMarblestone Grp. LLC, No. 18-CV-2727, 2020 WL 2745740, at *1 (E.D. Pa. May 27, 2020). The service provider alleged that the company (in this case a law firm) was the plan administrator and was careless by allowing its employees to work remotely and use their personal email accounts to conduct official business. This permitted the cybercriminal to steal the funds. The Court highlighted the split among the Circuits, where the 2nd and 7th Circuits permit co-fiduciaries to assert claims for contribution and indemnity, while the 8th and 9th Circuits hold, they do not.

Risk Mitigation

Fiduciaries are not experts in cybersecurity, nor are they law enforcement, that's why we have the FBI and various federal agencies. Nonetheless, from the investigations by the DOL and private litigation that has ensued, fiduciaries should take actions to mitigate their risks.

First, fiduciaries should ascertain whether they are adequately insured to address a cybercrime. Note that the ERISA fidelity bond is for a theft from insiders not outside cybercriminals. *See* Jara and Geary, *Is It Time for ERISA to Be Amended to Cover Cyber Crimes*, Tax Management Compensation Planning Journal, 50 CPJ 10, 10/07/2022 Furthermore, depending on how a case is pled, the fiduciary liability policy may or may not be triggered. Accordingly, it would be prudent to review and analyze the plan's insurance coverage and determine whether to obtain a separate cyber insurance policy to provide any gaps in coverage. Also, a cyber policy can provide coverage post breach (i.e., notification expenses, fixing the inability to use or damage to networks, and data recovery costs).

Second, fiduciaries should diligently negotiate service provider contracts and be mindful of the cybersecurity. This negotiation should result in cyber related contract provisions, including provisions that provide the right to review cybersecurity audit results and demonstrating compliance. Fiduciaries should inquire if the service provider is offering a guarantee of benefits, if a participants' account is hacked through no fault of their own.

In addition, fiduciaries can take the following actions:

- Learn more about fiduciary responsibilities as they relate to cybersecurity
- Assess their own cyber program, in addition to that of all the service providers —and—
- Educate participants about cyber risks.

In conclusion, while the days of fearing bank robbers disguised as Santa Claus are long gone, a cyber threat and many of its unknown disguises remains. The DOL in investigating plans has as made it clear this is something they are looking into. The litigation landscape shows that cases survive motions dismiss. And fiduciaries, while not cyber cops, should address cybersecurity to mitigate the risks of theft of plan assets as well as claims of ERISA breach of fiduciary duty against them.

In my next ERISA cyber related article, I will cover how the fiduciary obligations play out in a theft of plan data scenario. Stay tuned.

Related Content

Resource Kits

- Cybersecurity for Retirement Plans Resource Kit

Cases

- Disberry v. Emp. Rels. Comm. of the Colgate-Palmolive Co., 646 F. Supp. 3d 531 (S.D.N.Y. 2022)
- Walsh v. Alight Sols. LLC, 44 F.4th 716 (7th Cir. 2022)
- Leventhal v. MandMarblestone Grp. LLC, No. 18-2727, 2020 U.S. Dist. LEXIS 219942 (E.D. Pa. 2020)

José M. Jara, Counsel, Fox Rothschild LLP

José focuses his practice on the Employee Retirement Income Security Act (ERISA) and employment litigation and counseling. He has extensive experience in representing corporations, tax-exempts, associations, pension funds, boards of trustees, Employee Stock Ownership Plans (ESOPs), defined benefit and defined contributions plans, multiple employer plans, multiemployer plans, and executives in areas of employment, ERISA, and other employee benefits law matters.

José's practice includes representing clients under investigation by the U.S. Department of Labor's (DOL) Employee Benefits Security Administration and defending clients from lawsuits filed by DOL's Office of the Solicitor regarding civil and/or criminal violations of ERISA.

He defends plan sponsors, boards of directors and fiduciaries against ERISA class action litigation alleging breach of fiduciary duty under ERISA, including excessive fees, imprudent investments, delinquent employee contributions and improper valuation of employer stock. In addition, José provides legal advice to plan sponsors and fiduciaries on fiduciary responsibilities, plan fees and expenses, plan asset regulations and ERISA-prohibited transactions and exemptions.

He also works with clients to correct retirement plan errors under the IRS Employee Plans Compliance Resolution System, fiduciary violations under the DOL Voluntary Fiduciary Correction Program and annual reporting failures under the DOL Delinquent Filer Voluntary Compliance Program.

José advises clients on a broad range of labor and employment law issues such as wrongful termination, sexual harassment and discrimination, restrictive covenants, retaliation and matters related to labor law such as grievances, arbitrations and collective bargaining. He also defends companies against EEOC charges and DOL wage and hour investigations, conducts interactive harassment training, carries out internal investigations and drafts employment and severance agreements.

In addition, José assists clients with professional liability insurance matters, providing legal counsel on Directors & Officers (D&O), fiduciary and Employment Practices Liability (EPL) insurance issues. He has served as monitoring and coverage counsel and provided legal advice to underwriters on a variety of provisions of the insurance policy.

José speaks frequently on ERISA and employment law topics. He recently delivered presentations on DOL and IRS Health and Welfare Plan audits, Fiduciary Issues in ESG Investing, ERISA Prohibited Transactions and Exemptions, 2021 Employment Law Issues on the Enforcers' Radar, ESOP challenges and enforcement activity, and sexual harassment in the workplace, among other subjects.