Bloomberg Tax

Tax Management
Compensation Planning Journal™

Is It Time for ERISA to Be Amended to Cover Cyber Crimes?

By José M. Jara and Kelly Geary
Fox Rothschild LLP and Epic Insurance Brokers and Consultants
Morristown, NJ and Greenwich, CT

Back in the olden days, people were concerned about bank robberies. In fact, in response to a reporter's query as to why he robbed banks, a famous bank robber once stated: ''because that's where the money is.''[1] Fast forwarding to today's times, it is no surprise that cyberattacks are a grave concern for sponsors of retirement plans because the assets therein total $33.7 trillion (as of the second quarter of 2022).[2]

Under the Employee Retirement Income Security Act (ERISA),[3] fiduciaries and persons handling funds must be bonded to protect against fraud and dishonesty. This article will discuss this required ERISA bond and the interplay of other types of insurance coverage, and conclude with a recommendation that Congress amend ERISA to require insurance to address cyber crimes.

ERISA FIDELITY BOND

The U.S. Department of Labor, Employee Benefits Security Administration (the ''DOL'' or ''EBSA'') is entrusted with enforcing the provisions of Title I of ERISA. Title I was enacted to address public concern that funds of private pension plans were being mismanaged and abused.[4] Accordingly, several sections of ERISA go beyond civil mismanagement and address fraud and dishonesty.

---

[*] José M. Jara, counsel at Fox Rothschild LLP, focuses his practice on ERISA and employment litigation and counseling, including representing clients under investigation by the Department of Labor Employee Benefits Security Administration and defending them from lawsuits alleging violations of ERISA.

Kelly Geary is a managing principal with EPIC Insurance Brokers and Consultants. Kelly serves as the National Practice Leader — Executive and Cyber Risk.

This article may be cited as José M. Jara and Kelly Geary, *Is It Time for ERISA to Be Amended to Cover Cyber Crimes?*, 50 Tax Mgmt. Comp. Plan. J. No. 10 (Oct. 7, 2022).

[1] FBI History Famous Cases and Criminals — Wille Sutton.

[2] See the Investment Company Institute Report stating that:

> Assets in individual retirement accounts (IRAs) totaled $11.7 trillion at the end of the second quarter of 2022, a decrease of 11.4% from the end of the first quarter of 2022. Defined contribution (DC) plan assets were $9.3 trillion at the end of the second quarter, down 11.4% from March 31, 2022. Government defined benefit (DB) plans — including federal, state, and local government plans — held $7.3 trillion in assets as of the end of June 2022, a 6.9% decrease from the end of March 2022. Private-sector DB plans held $3.2 trillion in assets at the end of the second quarter of 2022, and annuity reserves outside of retirement accounts accounted for another $2.2 trillion.

[3] Pub. L. No. 93-406.

[4] History of EBSA and ERISA. When passing ERISA, the debates in Congress reveal, one main concern was to prevent the abuses in the management of plan assets by plan administrators:

> (''[I]nstances have arisen in which pension funds have been used improperly by plan managers and fiduciaries. . . . [T]his bill contains measures designed to reduce substantially the potentialities for abuse'') (remarks of Sen. Nelson), reprinted in 3 Leg. Hist. 4803; 120 Cong. Rec. 29957 (1974) (''In addition, frequently the pension funds themselves are abused by those responsible for their management who manipulate them for their own purposes or make poor investments with them'') (remarks of Sen. Ribicoff), reprinted in 3 Leg. Hist. 4811; 120 Cong. Rec. 29957 (1974) ''[M]isuse, manipulation, and poor management of pension trust funds are all too frequent'') (remarks of Sen. Ribicoff), reprinted in 3 Leg. Hist. 4812; 120 Cong. Rec. 29961 (1974)).

Mass. Mut. Life Ins. Co. v. Russell, 473 U.S. 134, 141, n.8 (1985).

ISSN 0747-8607

In particular, ERISA §412(a), subject to certain exceptions, requires that:[5]

> [e]very fiduciary of an employee benefit plan and every person who handles funds or other property of such a plan . . . shall be bonded as provided in this section . . .
>
> Such bond shall provide protection to the plan against loss by reason of acts of fraud or dishonesty on the part of the plan official, directly or through connivance with others. Any bond shall have as surety thereon a corporate surety company which is an acceptable surety on Federal bonds under authority granted by the Secretary of the Treasury pursuant to sections 9304–9308 of Title 31. Any bond shall be in a form or of a type approved by the Secretary, including individual bonds or schedule or blanket forms of bonds which cover a group or class.

It is unlawful for any person receiving, handling, disbursing, or otherwise exercising custody or control of any of the funds or other property[6] of any employee benefit plan.[7] It is further unlawful for a fiduciary to permit any person handling funds to not be bonded.[8] Thus, not only are fiduciaries and other employees at the sponsor required to be covered by the bond, but so are service providers.[9]

ERISA §412(e) authorizes the Secretary of Labor to prescribe regulations to carry out the bonding requirementand to exempt plans from the bonding requirement in specified situations.

The DOL promulgated 29 C.F.R. §2550.412-1, pending issuance of permanent bonding regulations implementing ERISA §412, which incorporates by reference most of the bonding regulations issued under the predecessor statute, the Welfare and Pension Plans Disclosure Act (WPPDA) and makes them applicable to plan officials under ERISA. In addition, the DOL issued FAB 2008-04, which provides guidance in a question-and-answer format for the DOL's Regional Enforcement Offices.

The DOL provides greater detail on what is considered ''handling'' which includes:[10]

- Physical contact. Physical contact with cash, checks or similar property.
- Power to exercise physical contact or control. Whether or not physical contact actually takes place, the power to secure physical possession of cash, checks, or similar property through factors such as access to a safe deposit box or similar depository, access to cash or negotiable assets, powers of custody or safekeeping, power to withdraw funds from a bank or other account generally.
- Power to transfer to oneself or a third party or to negotiate for value. With respect to property such as mortgages, title to land and buildings, or securities, while physical contact or the possibility of physical contact may not, of itself, give rise to risk of loss.
- Disbursement. Actual disbursement of funds or other property by persons such as officers or trustees authorized to sign checks or other negotiable instruments or to disburse cash.
- Signing or endorsing checks or other negotiable instruments. In connection with disbursements or otherwise, signing or endorsing checks or similar instruments or otherwise rendering them transferable, by any persons with the power to do so, whether individually or as co-signers with one or more other persons.
- Supervisory or decision-making responsibility. A person's supervisory or decision-making re-

---

[5] Legislative history states:

> It is the public policy of the United States, expressed in the Internal Revenue Code, in the Welfare and Pension Plans Disclosure Act and in other legislation, to support the growth of employee benefit plans and to protect the interests of participants in these plans. We believe that that policy is furthered by the legislative mandate that officers and employees of the plans be bonded.

ERISA-LH 19-A, 1973 WL 172974 (A.&P.L.H.), 461.

[6] The term ''funds or other property'' generally refers to all funds or property that the plan uses or may use as a source for the payment of benefits to plan participants or beneficiaries. 29 C.F.R. §2580.412-4. Thus, plan ''funds or other property'' can include:

- Employer and employee contributions that are received by the plan or otherwise paid out or used for plan purposes. 29 C.F.R. §2580.412-5(b)(2);
- All items in the nature of quick assets, such as cash, checks and other negotiable instruments, government obligations, marketable securities, and all other property or items that are convertible into cash or have a cash value that are held or acquired for the ultimate purpose of distribution to plan participants or beneficiaries; and
- All plan investments, even those that are not in the nature of quick assets, such as land and buildings, mortgages, and securities in closely held corporations. 29 C.F.R. §2580.412-4.

See DOL Field Assistance Bulletin (FAB) 2008-04, Q&A-17.

[7] ERISA §412(b).

[8] *Id.*; *Rosenbaum v. Hartford Fire Insurance Co.*, 104 F.3d 258, 263 (9th Cir. 1996) (''[t]he statute also prohibits plan officials from permitting any official who has not met the bonding requirements to receive, handle, disperse or control plan funds.'').

[9] DOL FAB 2008-04, Q&A-7, Q&A-8.

[10] 29 C.F.R. §2580.412-6.

ISSN 0747-8607

sponsibility to the extent it involves factors in relationship to funds discussed above.

The DOL also provides some guidance on the meaning of fraud or dishonesty as follows:[11]

> The term ''fraud or dishonesty'' shall be deemed to encompass all those risks of loss that might arise through dishonest or fraudulent acts in handling of funds as delineated in §2580.412-6. As such, the bond must provide recovery for loss occasioned by such acts even though no personal gain accrues to the person committing the act and the act is not subject to punishment as a crime or misdemeanor, provided that within the law of the state in which the act is committed, a court would afford recovery under a bond providing protection against fraud or dishonesty. As usually applied under state laws, the term ''fraud or dishonesty'' encompasses such matters as larceny, theft, embezzlement, forgery, misappropriation, wrongful abstraction, wrongful conversion, willful misapplication or any other . . . acts where losses result through any act or arrangement prohibited by title 18, section 1954 of the U.S. Code.

Through its regional offices, the DOL enforces what it believes the bond requirements are and what is a compliant bond.[12] DOL may assert that a bond is not compliant in regards to who is handling funds, amounts required,[13] coverage, and exclusions. Sometimes the regulations do not provide clear guidance. A plan sponsor or fiduciary will not (and should not) engage in any serious debate with the DOL. The quick fix is for the fiduciary to call their broker and request a compliant bond, addressing DOL's concerns.

Bonds generally exclude persons from being insured if they have committed acts of fraud or dishonesty in the past.[14] ERISA §411(a) provides further ERISA protections from crimes. It prohibits, in part, a person from serving as a fiduciary, trustee, or representative of any employee benefit plan in any capacity for 13 years after being convicted of a crime (as described in ERISA §411).[15] Note that ERISA §411(a)(3) bars such persons from having authority over the assets of the plan, but ERISA §411(a)(1) is much broader. Accordingly, such persons are barred whether they are handling plan assets or not, and violation of ERISA §411 itself is a crime.[16]

In a cyber breach scenario, the bond would not be triggered. In fact, the DOL's Advisory Council (the ''Council'') stated:[17]

> There was a consensus among the witnesses that today, losses to employee benefit plans due to theft, fraud, or dishonesty on the part of persons who handle plan funds or other property are far less significant than losses due to social engineering fraud and cybercrime. Fidelity bonds generally would not protect the plan against losses due to these latter risks because those losses do not result from theft, fraud or dishonesty by plan officials, but rather the fraudulent and criminal activity of outside parties.

Thus, unless a fiduciary was working through connivance with the cyber thieves, the bond would not be triggered.

CYBERSECURITY: WHAT'S THE FUSS ALL ABOUT?

A cyber incident is not a matter of if it will occur, but a matter of when.

For it is no longer a question of ''if,'' but ''when'' and ''how often.'' I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging

---

[11] 29 C.F.R. §2580.412-9; DOL FAB 2008-04, Q&A-1.

[12] Also note that the DOL requires the disclosure of a bond and its amount on Form 5500. IRS Form 5500, Schedule H, Part IV — Compliance Questions, Line 4e.

[13] For the amounts required see DOL FAB 2008-04, Q&A-35-42.

[14] DOL FAB 2008-04, Q&A-28.

[15] ERISA §411(a) crimes include:

> robbery, bribery, extortion, embezzlement, fraud, grand larceny, burglary, arson, a felony violation of Federal or State law involving substances defined in section 802(6) of title 21, murder, rape, kidnaping, perjury, assault with intent to kill, any crime described in section 80a-9(a)(1) of title 15, a violation of any provision of this chapter, a violation of section 186 of this title, a violation of chapter 63 of title 18, a violation of section 874, 1027, 1503, 1505, 1506, 1510, 1951, or 1954 of title 18, a violation of the Labor-Management Reporting and Disclosure Act of 1959 (29 U.S.C. 401), any felony involving abuse or misuse of such person's position or employment in a labor organization or employee benefit plan to seek or obtain an illegal gain at the expense of the members of the labor organization or the beneficiaries of the employee benefit plan, or conspiracy to commit any such crimes or attempt to commit any such crimes, or a crime in which any of the foregoing crimes is an element. . . .

[16] ERISA §411(b) provides that any person who intentionally violates this section shall be fined not more than $10,000 or imprisoned for not more than five years, or both.

[17] *See* Advisory Council on Employee Welfare and Pension Benefit Plans, Evaluating the Department's Regulations and Guidance on ERISA Bonding Requirements and Exposing Reform Considerations, p. 3 (Nov. 2018).

ISSN 0747-8607

into one category, companies that have been hacked and will be hacked again.[18]

According to The Boardroom Cybersecurity 2022 Report, published by Cybersecurity Ventures, cybercrime is predicted to cost the world $7 trillion in 2022. Cybersecurity for plans and insurers is a growing area of interest due to:

- Trying to protect trillions of dollars in plan assets;
- Breaches of personal identifiable information;
- Increased threat of large-scale cyberattacks;
- Lack of case law involving a cybersecurity breach and a retirement plan; and
- No federal regulation that directly protects retirement plans.

Further, as more plans begin to offer cryptocurrency as an investment option, the risk of cybertheft increases, making 401(k) accounts even more vulnerable. In 2022, bad actors turned their attention to crypto and the decentralized finance (DeFi) sectors. Cybercriminals have stepped up their efforts to steal funds by using various social engineering tactics. In August 2022, the FBI issued a warning about a potential spike in cyberattacks against cryptocurrency.

Unfortunately, for fiduciaries in charge of managing employee benefit plans, there is not any guidance in the form of regulations, which provides for a robust notice and comment process, including review by the Office of Information and Regulatory Affairs (OIRA).

In 2016, the Council examined cybersecurity considerations for employee benefit plans. The Council acknowledged that fiduciaries are challenged by limited resources and technical expertise as well as the lack of clear standards. As such, the Council recommended that fiduciaries consult cybersecurity experts to aid in the development of a cyber risk management program for its employee benefit plans.

The Council's report centers on the fiduciaries' burden on creating a risk management strategy,[19] advising that fiduciaries understand what cyber insurance does and does not provide and how it coordinates with other types of insurance coverage. However, it did not recommend that the DOL issue regulations.

While there are no regulations, the DOL provided guidance in the form of best practices for maintaining cybersecurity. The DOL issued the following:

- **Tips for Hiring a Service Provider:** Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.[20]
- **Cybersecurity Program Best Practices:** Assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks.[21]
- **Online Security Tips:** Offers online basic rules for plan participants and beneficiaries who check their retirement accounts to follow to reduce the risk of fraud and loss.[22]

Additionally, the General Accounting Office (GAO) recommended that the DOL: (1) formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans; and (2) establish minimum expectations for addressing cybersecurity risks in these plans.[23] DOL did not state whether it agreed or disagreed with the first recommendation, but it agreed with GAO's second one.

Recently, the Seventh Circuit Court of Appeals provided some guidance:[24]

> As the Supreme Court has long recognized, Congress incorporated into ERISA 'a standard of loyalty and a standard of care.' The reasonableness of [a service provider's] cybersecurity services, and the extent of any breaches, is therefore 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].

ERISA FIDUCIARY LIABILITY INSURANCE

A common fallacy is that the fidelity bond is the same as the ERISA fiduciary liability policy. But there is a fundamental difference in that the fidelity bond covers crimes such as theft and the fiduciary policy generally covers losses as a result of a breach of fiduciary duty.[25] Another difference is that the fidelity bond is required under ERISA, it cannot have a de-

---

[18] Robert S. Mueller, Director of the FBI (quote from speech given in 2012).

[19] Advisory Council on Employee Welfare and Pension Benefit, Cybersecurity Considerations for Benefit Plans (Nov. 2016).

[20] Employee Benefits Security Administration (EBSA), TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES.

[21] EBSA, CYBERSECURITY PROGRAM BEST PRACTICES.

[22] EBSA, ONLINE SECURITY TIPS.

[23] *See* GAO, DEFINED CONTRIBUTION PLANS: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans (Feb. 2021).

[24] *Walsh v. Alight Sols.*, 44 F.4th 716, 723 (7th Cir. 2022).

[25] DOL FAB 2008-04, Q&A-2.

ISSN 0747-8607

ductible, and it can be paid from plan assets.[26] On the other hand, the fiduciary liability policy is optional under ERISA. But if it is obtained, it is subject to ERISA §410. If the fiduciary liability policy is paid with plan assets, it must permit recourse by the insurer against the fiduciary in the case of a fiduciary breach.[27]

The fiduciary policy specifically excludes crimes from coverage. It's usually quite broad, excluding any claims of deliberate fraud or criminal act or willful criminal violation in any jurisdiction around the world. In a cybercrime scenario, the policy will not provide coverage.

CYBER INSURANCE

Cyber insurance may enable plan sponsors and service providers to recover some costs associated with an attack, but the extent of the recovery will depend on the facts and circumstances of the attack and the specific policy wording at issue. And, in most instances, cybercrime coverage is very limited or specifically excludes amounts stolen from participants' accounts.

Most comprehensive cyber insurance policies on the market today include affirmative coverage for cyber extortion/ransomware. In most instances, the policy will provide coverage for the costs of hiring a company to investigate, negotiate, and resolve the threat made against the insured entity. The coverage will also extend to the payment of the ransom, so long as such payment would not run afoul of any domestic or international sanctions.

Further, cyber policies provide for first-party expenses — that is, costs that organizations would ordinarily have to pay to mitigate losses related to a data breach or privacy incident. Below are the first-party costs typically covered in a comprehensive cyber insurance policy:

- **Notification Expenses:** Coverage for breach response services such as notification expenses, credit monitoring, identity/credit repair, and call center support services to respond to questions from clients/customers; typically, also includes costs to engage legal counsel to ensure response complies with relevant law.
- **Crisis Response:** Coverage for retaining a public relations/crisis management firm to help mitigate damage to the insured's reputation; includes costs of advertising and communications to help repair image/reputation.
- **Forensics:** Coverage for cost to investigate to determine the cause and extent of a network security breach and to identify/catalog names and addresses of impacted individuals for the purpose of providing notification.
- **Data Recovery Costs:** Coverage for costs incurred by the insured to restore information/data that is altered, corrupted, destroyed, or damaged as a result of a network security breach.

Cyber policies also provide coverage for third-party expenses — that is, costs associated with defending liability claims and/or fines and penalties assessed by regulating authorities. Specifically, these costs may include:

- **Civil Liability — Network Security/Privacy Liability:** Coverage for civil liability claims arising from the alleged failure of network security to prevent the transmission of a malicious code or viruses, or other penetration of the computer system by an unauthorized user (hacker or rogue employee) and/or failure to protect non-public personal or corporate information in any format (electronic or hard copy).
- **Regulatory Defense and Fines/Penalties:** Coverage for regulatory proceedings brought by, or on behalf of, a governmental or regulatory authority to enforce privacy laws or regulations. Coverage is available for defense of the investigation or proceeding as well as fines/penalties awarded, to the extent such are insurable under relevant law.

While most comprehensive cyber insurance policies do provide coverage for various types of ''cybercrime,'' the coverage is typically very narrow and subject to low limits. One of the more popular cyber policy coverages addresses ''Social Engineering Fraud'' (SEF). SEF is typically described as the intentional misleading of an employee into transferring money or making a payment to a cyber-criminal based on fraudulent information provided to, and relied upon by, that employee. This is an incredibly difficult risk for underwriters to evaluate, accordingly, the coverage offered is very narrow. The limits of coverage offered vary based on underwriting criteria but, for an average risk, limits range from about $100,000 to $250,000, with deductibles/retentions often set at an amount equal to the limit. The coverage itself is very narrowly drafted and, in most cases, only applies to the insured entity's ''money,'' not to money the insured is holding or managing for a third party.

As a general proposition, a cyber policy is intended to cover losses related to data/information. Whereas a commercial crime policy is intended to protect against

[26] *Id.* at Q&A-11 and Q&A-30.

[27] *Id.* at Q&A-2.

ISSN 0747-8607

direct loss of money, securities, or tangible property (typically not data) caused by employees as well as outside third parties.

RECOMMENDATION: MANDATE COMMERCIAL CYBER CRIME COVERAGE

Federal law is unclear about who is responsible for losses associated with cybertheft of plan assets. Although many believe the custodians of the plan will reimburse when there are such instances of fraud/theft, that is not always the case. Every situation will present with different facts. There is no specific or comprehensive insurance product that will respond. This could leave individual plan participants in an untenable situation pursuing recovery of plan assets in the court system for years with no certainty of recovery and at huge personal expense.

While it is a good idea for fiduciaries to address at board meetings how various insurance types of coverage mitigate risks to the plans they manage, these insurance programs won't be comprehensive unless there's a component to address cybercrime. Fiduciaries are entrusted to manage plans under the duty of prudence and loyalty. They are not and should not be placed in the position of acting as criminal law enforcement.

Instead of burdening fiduciaries with yet another important item to think about in managing a plan, Congress can amend ERISA and mandate that the fiduciaries take out a policy to cover cybercrimes committed by third parties. Such amendment should lay out the amount of coverage, who is covered, and important miscellaneous details, or require the Secretary of Labor to issue regulations.

ISSN 0747-8607