EMPLOYEE BENEFITS

Society of FSP™ Financial Service Professionals

AUGUST 2021

Cybersecurity and Related Legal Risks Come Home to ERISA Plans

George Michael Gerstein

ERISA-covered plans have entered the digital world. As the amount of confidential information about plan participants that is stored in multiple information systems, and shared among plan service providers, increases, so, too, do the legal risks. The U.S. Department of Labor (DOL) has now made cybersecurity risk an enforcement priority; the courts have started to wrestle with whether participant data is a "plan asset." Plan sponsors and service providers should brace themselves.

Just this past February, the U.S. Government Accountability Office (GAO) issued a report that highlighted the practice of, and risks related to, sharing personally identifiable information (e.g., a participant's Social Security number, date of birth, and username/password) (PII), and "plan asset data" (e.g., retirement account and bank account numbers) within the plan ecosystem. The plan sponsor's own IT infrastructure may be vulnerable to attack or misuse.

INSIDE THIS ISSUE

Where the plan sponsor outsources plan administrative responsibilities to a service provider, such as recordkeepers, third-party administrators, and custodians, participant PII and plan asset data could be exploited if the service provider is hacked or lacks appropriate internal controls.

The report specifically noted that cybersecurity risk comes in many different flavors and from many different sources. The risk could, for example, be in the form of malware, ransomware, privilege abuse, data exfiltration, and account takeover. The source of the risk could come from criminal syndicates, hackers, and even an organization's own employees.

Thus, the GAO report warned, "[t]he sharing and storing of this information can lead to significant cybersecurity risks for plan sponsors and their service providers, as well as plan participants." Poor risk controls can lead to the leaking of usernames, passwords, and Social Security numbers, which can lead to the unauthorized access of participant accounts, and, fatally, the illicit draining of a participant's retirement savings. The misappropriation of participant PII or plan assets by virtue of a cybersecurity attack may not be expressly addressed in ERISA, but its effect on a participant may indeed result in "the great personal tragedy" Congress sought to prevent in enacting ERISA.[1]

The GAO ultimately made two recommendations: (1) the DOL should formally state whether cybersecurity for ERISA-covered retirement plans is a plan fiduciary responsibility under ERISA; and (2) the DOL

continued on page 2

Cybersecurity

continued from page 1

should develop and issue guidance that identifies minimum expectations for mitigating cybersecurity risks to plans and the relevant service providers.

A mere 2 months later, the DOL issued a series of cybersecurity tips and best practices for plan sponsors, service providers, and participants. Specifically:

- **Tips for Hiring a Service Provider,*** to "help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires."
- **Cybersecurity Program Best Practices,**** to "assist plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks."
- **Online Security Tips,***** to "offer plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss."

Useful as the tips and practices may be, the big reveal is that the DOL indicated that ERISA's duty of prudence encompasses "an obligation to ensure proper mitigation of cybersecurity risks." This means that a responsible plan fiduciary, when determining whether to hire and retain a service provider, should consider the service provider's cybersecurity risk controls, and should document such consideration as part of its overall evaluation of the service provider.

The upshot of the DOL's April 2021 cybersecurity tips and best practices is that it puts employers on notice that both the DOL takes this seriously and that plaintiffs could attempt to use this new guidance as a basis for fiduciary duty breach claims. Moreover, service providers can expect detailed questions on cybersecurity in RFPs and RFIs. Plan sponsors will seek more transparency, whereas service providers may be reluctant to divulge too much on their cybersecurity defenses to guard against inadvertently offering up the keys to the castle. The balance of the two will become market practice.

The DOL is ramping up enforcement in this area. Plan sponsors should also gird for class-action lawsuits with allegations of breaches of ERISA's duty of prudence when participant PII or plan asset data is misused. For these reasons, employers and plan service providers should carefully consider the DOL guidance.

A related string of litigation also poses a risk to plan sponsors and service providers. These suits argue that participant PII and plan asset data constitute "plan assets," and that using such data for marketing purposes amounts to a breach of fiduciary duties. Some of these suits have targeted both the plan's sponsor and recordkeeper. So far, the courts have rejected these claims.

In one case,[2] plaintiffs brought an action against the plan sponsor and recordkeeper alleging that participant data (e.g., names, contact info, investment history, etc.) constituted plan assets, and, therefore, the recordkeeper's purported sharing of this information with affiliates to cross-sell nonplan retail financial products to participants amounted to violations of ERISA. In granting the recordkeeper's motion to dismiss, the court ruled that "participant data does not meet the statutory definition of 'plan assets'...."

In a similar case,[3] plaintiffs brought suit against the plan administrator alleging, *inter alia,* breach of fiduciary duty over the plan's recordkeeper access to participant information (e.g., investment choice, account size, etc.) *and* use of that data to market products to the participants. In granting the motion to dismiss, the court stated, "[p]laintiffs cite no case in which a court has held that such information is a plan asset for purposes of ERISA....[t]his Court does not intend to be the first." Moreover, the court rejected the argument that "releasing confidential information or allowing someone to use confidential information constitutes a breach of fiduciary duty under ERISA."

Cybersecurity is quickly becoming an important risk area for ERISA plan sponsors. Protection of participant PII and plan asset data against privilege abuse, account takeovers, and other vulnerabilities

continued on page 8

DOL Says Claimant May Request Phone Call Recordings Relevant to Benefits Claim

Alexander Olsen

The DOL has stated in a June 14, 2021, Information Letter, that under ERISA claims procedures, a participant must be given audio recordings of telephone conversations that are relevant to his claim for benefits.

Background

The participant requested a copy of an audio recording of a telephone conversation with the plan's insurer relating to an adverse benefit determination. The plan and insurer denied the request for the recording, saying that the recordings are for "quality assurance purposes," and "are not created, maintained, or relied upon for claim administration purposes, and therefore are not part of the administrative record."

DOL Information Letter

In its information letter, the DOL noted that ERISA requires every employee benefit plan to "afford a reasonable opportunity to any participant, whose claim for benefits has been denied, for a full and fair review by the appropriate named fiduciary of the decision denying the claim." The regulations further say that a plan's claims procedures do not provide for a full and fair review, unless, among other things, the claimant is "provided, upon request…with copies of, all documents, records, and other information relevant to the…claim for benefits."

For this purpose, the DOL explained that a document, record, or other information is "relevant" to a claim if it: (i) was relied upon in making the benefit determination; (ii) was submitted, considered, or generated in the course of making the benefit determination, without regard to whether such document, record, or other information was relied upon in making the benefit determination; (iii) demonstrates compliance with the administrative processes and safeguards; or (iv) constitutes a statement of policy or guidance with respect to the plan concerning the denied treatment option or benefit for the claimant's diagnosis.

Further, the DOL clarified that nothing in the regulation requires that "relevant documents, records, or other information" consist only of paper or written materials. An audio recording can be part of a claimant's administrative record.

Therefore, the DOL concluded that a recording of a conversation with a participant would not be excluded from disclosure merely because the plan or claims administrator does not include the recording in its administrative record; does not treat the recording or transcript as part of the claim activity history through which the insurer develops, tracks, and administers the claim; or because the recording or transcript was generated for quality assurance purposes. ■

DOL Information Letter 06-14-2021 is available at: https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/information-letters/06-14-2021.

Alexander Olsen, Esq., is a partner with The Wagner Law Group in Boston where he specializes in the fields of ERISA and employee benefits law.

Does the Tail Know What the Head is Doing?

The Importance of Internal Communication between Management and Employee Benefits Personnel

Jordan Schreier

Employers who sponsor employee benefits plans are used to providing ongoing communication to plan participants. The communications range from legally required disclosures (e.g., summary plan descriptions) to legally required notices (e.g., COBRA notices) to information voluntarily provided to participants (e.g., the importance of saving for retirement). However, regular internal communication between employer management and employees responsible for benefit plan administration and compliance ("benefits staff") is also vital to the effective operation of an employee benefits program. A lack of effective communication between an employer's management and benefits staff can result in costly, yet avoidable, compliance violations, employee relations issues, and other problems.

Here are four examples of the importance of effective internal communication between employer management and benefits staff.

1. Change in Employer Aggregation Group Members

Employers regularly purchase or sell entities that are required to be aggregated with the employer and treated as a single employer with it under the controlled group, trades or businesses under common control, and/or affiliated service group rules. By way of example, some form of employer aggregation applies for purposes of:

- Nondiscrimination rules that apply to qualified retirement plans
- Nondiscrimination rules that apply to cafeteria plans and dependent care spending account plans
- The applicable large employer rules under the Affordable Care Act's employer shared responsibility rules
- The small-employer exception to COBRA
- The comparable health savings account contribution rules
- Determining who is the service recipient under the deferred compensation rules of Internal Revenue Code Section 409A
- Determining what entities constitute the employer subject to joint and several liability under the multiemployer withdrawal liability rules.

Sometimes management closes a sale or acquisition transaction but does not inform benefits staff or only does so months or years later. This may occur for a variety of reasons, such as the acquired business maintaining its own benefits programs that will not be integrated with the acquirer's benefit plans; the transaction being conducted overseas and primarily involving foreign entities with a U.S. entity being a small portion of the transaction; or a perceived need for confidentiality before and after the transaction.

A common theme in many of these situations is management not being familiar with the employer aggregation rules or their importance for benefit plan compliance.

Fortunately, not recognizing the employer aggregation impact of a transaction does not always result in a compliance violation. For example, Code Section 410(b) includes a transition period during which a qualified retirement plan is treated as continuing to comply with the code's minimum coverage rules for a period of time after a transaction, provided the plan complied immediately prior to the transaction, and certain other conditions are satisfied. However, other rules, such as the cafeteria plan rules, do not include any transition relief.

It is important for employer management to understand the employer aggregation rules and to communicate early with benefits staff so that they can help management structure transactions to maximize compliance with the employer aggregation rules.

2. Change in Ownership Percentages without Change in Employer Aggregation Group Members

Sometimes even a sale or acquisition of a small percentage of a business that results in no change to an employer aggregation group can impact benefits

compliance. For example, an employer that maintains a multiple employer welfare arrangement ("MEWA") (generally an employee welfare plan that provides benefits to employees of two or more employer groups) is not required to file with the Department of Labor an annual Form M-1 report for the MEWA as long as the employers participating in the plan share a common control interest of 25 percent or more during the plan year. For a common control group slightly above the 25 percent threshold, the filing exemption can be lost due to a small percentage ownership change that has no impact on employer aggregation (though there is limited transition relief from immediate Form M-1 filing responsibility). Again, communication between employer management and benefits staff about even a small transaction can avoid costly and complicated legal compliance violations down the road.

3. Special Benefit Promises

An important time for management to consult with benefits staff is when the employer is considering making special benefit promises to an employee. This can occur in connection with an employee termination when an employer agrees to continue the terminated employee's benefits for a few months post-termination generally or as part of a separation agreement. Management may not know that some benefits, such as insured long-term disability and life insurance, may not simply be continued for a former employee, risking the employer having to self-fund disability or death benefits in the event of an uninsured claim. Another situation in which advance communication can prevent a violation is with verbal promises of deferred compensation to an employee. Code Section 409A requires deferred compensation agreements to be in writing and include certain provisions such as the manner and timing of payment. A brief consultation with benefits staff when special benefit terms are being considered could prevent potentially costly liability.

4. Decisions to Change Benefits Made at Board Meetings or in Collective Bargaining

The decision to revise the terms of an employee benefits program can occur in a variety of ways. For example, decisions may be made at a board of directors meeting or as a result of collective bargaining. Compliance violations can occur when there is a delay between when these benefit change decisions are made and when benefits staff is informed of the changes, and the longer the delay, the greater the risk. For example, some benefit changes cannot have a retroactive effective date (reductions in plan required employer nonelective contributions to a defined contribution plan where no minimum service requirement applies) or can only be effective as of the first day of a plan year (e.g., certain changes to the terms of a safe harbor 401(k) plan).

Other changes require a specific advance notice period before the change can be effective (certain changes in group health plan terms). In addition, third-party service providers typically require some minimum advance notice so they can adjust their benefit administration systems. When management does not promptly advise benefits staff of agreed-to changes to plan terms, it puts benefits staff in the unenviable position of having to let management know their decisions cannot be implemented as planned. It can also result in employer financial cost and union/employee relations problems.

Takeaways

The importance of effective internal communication between employer management and benefits staff cannot be overstated. Benefits staff are an employer's front line for knowledge of employee benefit plan terms and conditions, requirements under third-party service provider contracts, and compliance with the many laws that impact an employee benefits program. Optimally, employer management will consult with benefits staff prior to making business decisions, such as the acquisition or sale of a business entity, which may affect their employee benefit plans' terms or ability to comply with the law. If that is not possible, employers should inform benefits staff of decisions promptly after they are made, so benefits staff can take the steps necessary to implement the decision, keep the plans legally compliant, and protect the employer from potentially costly and disruptive liability. In the employee benefits world, the old saying "the head doesn't know what the tail

continued on page 6

Are Your COBRA Notices Sufficient to Avert a Costly Challenge?

Randy Scherer and Lisa Van Fleet

While the Consolidated Omnibus Budget Reconciliation Act (COBRA) continuation coverage subsidy requirements imposed by the American Rescue Plan Act of 2021 are at the forefront of employers' minds, recent litigation trends should motivate plan sponsors to review their standard COBRA election notices to ensure they comply with the general requirements in the regulations promulgated by the Department of Labor (DOL).

The regulations[1] require COBRA notices be written in a manner calculated to be understood by the average plan participant. Required information includes:

- The name and plan under which continuation coverage is available;
- The name, address, and phone number of the plan administrator;
- Identification of the qualifying event;
- Identification of the qualified beneficiaries (by status or name) who are recognized by the plan as being entitled to elect continuation coverage due to the qualifying event;
- An explanation of the procedures for electing coverage, and the consequences of failing to elect coverage;
- A description of the coverage available;
- The time period for which the coverage is available; and
- The cost of coverage and due dates for payments.

A spate of recent litigation reminds us that failure to include required information in COBRA election notices may expose the plan sponsor and the plan administrator to claims from participants and beneficiaries. Further, if the information included in COBRA election notices is likely to confuse participants and beneficiaries, there may be potential liability for failure to provide a notice written in a manner calculated to be understood by the average plan participant.

In *Green v. FCA US LLC*[2], the plaintiffs alleged that the COBRA election notices sent by the defendants were deficient because they included an "ominous warning" that suggested plaintiffs could be subject to civil and criminal penalties if they submitted incorrect, or even incomplete, information when electing COBRA. According to the plaintiffs, this warning was unnecessary, and it "confused and discouraged them, at least in part" from electing COBRA continuation coverage. The plaintiffs also alleged that the notices failed to identify the name and contact information of the plan administrator.

In an order granting in part and denying in part the defendants' motion to dismiss, the court determined that the failure to include the name and contact information of the plan administrator was a "bare procedural violation, divorced from any concrete harm" to the plaintiffs, as they did not allege an injury-in-fact based

Communication

continued from page 5

is doing" is reversed. The benefits staff tail needs to know what the management head is doing. ■

This article was originally published by Dickinson Wright PLLC on its All Things HR *blog. It is reprinted with permission. Copyright © 2021 by Dickinson Wright PLLC.*

Jordan Schreier is a member in Dickinson Wright's Ann Arbor office and chair of the firm's Employee Benefits and Executive Compensation Practice Group. His practice involves advising both for-profit and nonprofit employers on planning and compliance issues involving all aspects of employee benefits, including welfare benefits, qualified retirement, and other deferred compensation plans.

on this failure. The court dismissed the claim based on this failure due to lack of standing under Article III.

However, the court denied the defendants' motion to dismiss the claim based on the warning regarding potential civil and criminal penalties for submitting incorrect or incomplete information. The court held that the plaintiffs had plausibly alleged the notice was not written in a manner calculated to be understood by the average plan participant, as the assertion that participants could be subject to penalties for providing *incomplete* information was not a "strictly accurate statement of the law."

Several other recent claims regarding defective COBRA election notices have ended in settlement. By way of example, the court in *Holmes v. WCA Mgmt. Co., L.P.*[3] recently approved a Joint Motion for Preliminary Approval of Class Action Settlement in the amount of $210,000. In *Holmes,* the plaintiffs alleged the defendants provided deficient COBRA notices that (1) failed to provide and explain the continuation coverage termination date; (2) failed to include information regarding how COBRA coverage can be lost before the omitted termination date; (3) failed to identify the plan administrator for the group health plan; and (4) was not written in a manner calculated to be understood by the average plan participant. Currently, there are COBRA election notice cases pending against Amazon[4] and Starbucks[5], among others.

Plan sponsors should take steps to ensure their COBRA notices meet all of the requirements found in the DOL regulations. The DOL has provided model COBRA notices that may be used, and use of such notices, when properly completed, will be considered good faith compliance with COBRA notice requirements.

For plan sponsors opting not to use the DOL model notices, comparing the notices that are used against the model notices is advisable. Plan sponsors should also consider some of the common pitfalls that have given rise to recent COBRA notice litigation, taking particular care to:

- Include the group health plan administrator and contact information, as well as important deadlines and the process for electing coverage;
- Review notice language to ensure it is clear and is not likely to mislead or confuse participants;
- Issue the notice within the required timeframe, typically within 14 days of receiving notice of a qualifying event for the COBRA election notice;
- Provide notices in Spanish (or other appropriate language) for employees who primarily speak Spanish (or such other language); and
- Review regulations, guidance, and model notices to ensure all required information is included, or have employee benefits counsel do so.

While plan sponsors are understandably preoccupied with the new COBRA responsibilities imposed by recent legislation, they should take this as an opportunity to carefully review their standard COBRA notices. Following the simple steps outlined above will go a long way towards accomplishing that vital review and may prevent potentially costly headaches down the line. ■

This article was original published in the BCLP Benefits *newsletter by Bryan Cave Leighton Paisner and is reprinted with permission.*

Randy Scherer is an associate in Bryan Cave Leighton Paisner's Employee Benefits and Executive Compensation group, where he often advises on compensation and benefits matters in the context of mergers and acquisitions. Randy currently serves as the chair-elect for the Employee Benefits Section of the Bar Association of Metropolitan St. Louis.

As a highly experienced partner with Bryan Cave Leighton Paisner LLP, Lisa Van Fleet counsels employers on all aspects of retirement and welfare plans and deferred and equity-based compensation, with particular emphasis on implementation of best practices to minimize fiduciary and litigation exposure. A fellow with the American College of Benefits Counsel, Lisa is a frequent speaker and writer on employee benefits and holds leadership positions with the American Bar Association and the national TE/GE Council.

(1) 29 CFR 2590.606-4(b)(4).

(2) Case No. 2:20-cv-13079-GCS-DRG (E.D. Mich. 2021).

(3) Case no. 6:20-cv-698-PGB-LRH (M.D. Fla. 2021).

(4) *Kendall v. Amazon Corporate, LLC,* case no. 3:20-cv-02493 (D.S.C. 2020).

(5) *Torres v. Starbucks Coffee Company,* case no. 8:20-cv-01311 (M.D. Fla. 2020).

Cybersecurity

continued from page 2

to a participant's information and account raises the specter for DOL enforcement action and litigation. Service providers should anticipate a greater focus on their cybersecurity measures by plan sponsors and expect that such measures could be an important basis to be hired and retained as a plan service provider. Both employers and plan service providers should also consider whether it is complying with other applicable privacy laws (to the extent such laws are not preempted by ERISA). ■

This article was originally published by Stradley Ronon and is reprinted with permission. Copyright © 2021 by Stradley Ronon. All rights reserved.

George Michael Gerstein, Esq., practices in Stradley Ronon's Washington, D.C. office where he advises plan sponsors and financial services firms on the fiduciary and prohibited transaction provisions of ERISA and the rules and regulations applicable to governmental plans. He's also cochair of the fiduciary governance and ESG groups.

(1) *Nachman Corp. v. PBGC,* 446 U.S. 359, 374, 100 S. Ct. 1723, 1733, 64 L. Ed. 2d 354, 366 (1980).

(2) *Harmon v. Shell Oil Co.,* No. 3:20-cv-00021, 2021 BL 126207 (S.D. Tex. Mar. 30, 2021).

(3) *Divane v. Northwestern Univ.,* No. 16 C 8157, 2018 BL 186065 (N.D. Ill. May 25, 2018), aff'd, 953 F.3d 980 (7th Cir. 2020).

*Tips for Hiring a Service Provider with Strong Cybersecurity Practices (dol.gov); https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf.

**Cybersecurity Program Best Practices (dol.gov); https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

***Online Security Tips (dol.gov); https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.

EMPLOYEE BENEFITS is published four times a year by and for Employee Benefits Section members. This newsletter is designed to provide a forum for ideas and topics pertinent to employee benefits. Statements of fact or opinion are the responsibility of the authors and do not represent an opinion on the part of committee members, officers, individuals, or staff of the Society of Financial Service Professionals.

Editor Anne Rigney, JD, CLU, ChFC
Society of FSP™
610-526-2536
arigney@SocietyofFSP.org

10 E. Athens Avenue, Suite 224
Ardmore, PA 19003
Tel: 610-526-2500 • Fax: 610-359-8115
Website: www.SocietyofFSP.org

Society of FSP™
Financial Service Professionals