THE WAGNER LAW GROUP

99 Summer Street, 13th Floor
Boston, MA 02110
Tel. 617-357-5200
www.wagnerlawgroup.com

September 30, 2020

By E-mail: wilson.jeanne.k@dol.gov
and via Certified Mail – Return Receipt Requested

Jeanne Klinefelter Wilson
Acting Assistant Secretary
Employee Benefits Security Administration
United States Department of Labor
200 Constitution Avenue NW S-2524
Washington, DC 20210

Re: Cybersecurity Measures and Participant Personal Information

Dear Acting Assistant Secretary Wilson:

As the practice of benefit plans storing and transmitting participant personal information ("PPI") electronically has increased, occurrence of cyberbreaches has grown exponentially. There is an acute need for comprehensive guidance from the U.S. Department of Labor (the "Department") with respect to fiduciary responsibilities under the Employee Retirement Income Security Act of 1974, as amended ("ERISA"), to protect against the unauthorized withdrawals from participants' accounts and how fiduciary responsibilities extend to protection against the unauthorized appropriation of PPI, and the measures plan fiduciaries, and indirectly plan service providers, are required to take to achieve this ("cybersecurity").[1] This need is urgent given the pervasiveness of cybersecurity threats that will only increase against employee benefit plans as demonstrated in recent well publicized cases of unauthorized withdrawals from 401(k) plans.[2] Recognizing the risk, lawmakers have asked the Government Accountability Office ("GAO") to examine the cybersecurity of the U.S. retirement system.[3] Moreover, the U.S. Securities and Exchange Commission ("SEC") recently issued a *Risk Alert* describing the increase in

[1] For purposes of this letter, the term "cybersecurity" encompasses the privacy of PPI. We understand that there may be implications for benefit plans under state privacy laws, which we raise later in this letter. We also recognize that participants in group health plans have privacy rights under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

[2] *Leventhal v. MandMarblestone Group. LLC*, No. 18-cv-2727 (E.D. Pa. May. 27, 2020) (motion to dismiss ruling that both plan administrator and TPA are jointly and severally liable if a fiduciary breach is proven); *Barnett v. Abbott Laboratories et al.*, No. 2020 CV 2127, (N.D. Ill. filed April 3, 2020); *Berman v. Estee Lauder Inc.*, No. 3:19-cv-06489, (N.D. Cal. filed October 9, 2019, settled in March 2020).

[3] Letter to the Comptroller General of the GAO from the House Committee on Education & Labor and the Committee on Health, Education, Labor & Pensions, dated February 12, 2019. It is our understanding that a report from the GAO may be forthcoming.

cyberattacks against registered investment advisers and broker dealers that resulted in the loss of customer assets or unauthorized access to customer information in some cases.[4]

Department's Limited Comments on Cybersecurity and PPI

Thus far, the Department has not taken a formal position on the cybersecurity of PPI. However, the Department's limited comments on this topic can be found in the final regulations on the electronic furnishing of certain required disclosures of employee retirement benefit plans subject to ERISA.

Prior to 2020

In 2002, the Department issued a final regulation at 29 CFR § 2520.104b-1(c) ("2002 Guidance") dealing with permissible electronic disclosures to plan participants and beneficiaries that required a plan administrator to take "appropriate and necessary measures reasonably calculated to ensure that the system for furnishing documents protects the confidentiality of the personal information relating to the individual's accounts and benefits."[5] In the preamble, the Department indicated that it was "not prepared at this time, however, to express any view as to the adequacy of any particular method to protect confidentiality, such as the use of PINs or passwords."[6]

In October 2019, the Department published a proposed rule and Request for Information (RFI) ("2019 Proposal") intended to expand the methods by which ERISA retirement plan disclosures may be furnished electronically. The 2019 Proposal would allow plan administrators who satisfy certain conditions to furnish the required disclosures electronically, or to notify participants and beneficiaries that certain disclosures will be made available on a Website, while preserving the right of these individuals to opt out of electronic delivery and to request paper copies of disclosures. One of the Website standards requires the plan administrator to "take measures reasonably calculated to ensure that the website protects the confidentiality of personal information relating to any covered individual." Question 18 of the RFI requested comments on cybersecurity issues associated with electronic disclosure,[7] but the response from commenters on this topic was not substantive.

---

[4] *Risk Alert*, Office of Compliance Inspections and Examinations, SEC, September 15, 2020: "Cybersecurity: Safeguarding Client Accounts Against Credential Compromise."

[5] 29 CFR § 2520.104b-1(c)(1)(B).

[6] 29 Fed. Reg. 17267 (April 9, 2002).

[7] 29 Fed. Reg. 56909 (October 23, 2019). "Some plan sponsors and participants have expressed concerns about cybersecurity and privacy when participants access sensitive plan information and engage in financial activity online. To protect against these concerns, how do plan administrators currently assess risks and provide secure online access to their participants? What safeguards are implemented to protect participants, how effective are they, and what improvements could be made to make current systems more secure? What cost considerations are raised by increasing cyber security and privacy protections? Should risk assessments and security measures be required by regulation?"

2020 Final Rule

The final regulation issued by the Department on March 27, 2020, that went into effect on July 27, 2020 ("2020 Final Rule"), does not replace the 2002 Guidance, but rather adopts a new, additional safe harbor for employee benefit retirement plan administrators to use electronic media as a default to furnish "covered documents" (disclosures under Title I of ERISA such as summary plan descriptions) to "covered individuals" *(i.e.,* participants, beneficiaries, and other individuals entitled to receive covered documents) of plans subject to ERISA. As in the proposal, the 2020 Final Rule provides two options by which plan administrators can electronically furnish or deliver retirement plan covered documents: (i) notice of access to a plan disclosure Website posting, and (ii) direct email disclosure. Under either option, "the administrator must take measures *reasonably calculated* to protect the confidentiality of personal information relating to any covered individual" when furnishing covered documents.[8] (emphasis added).

The requirement to take measures *reasonably calculated* to protect the confidentiality of PPI appears to be different from the prudence standard under ERISA Section 404,[9] which the Department specifically refers to in the 2020 preamble as providing an overall umbrella applicable to the protection of covered individuals' personal information. In acknowledging cybersecurity concerns and the increased risk to PPI posed by e-delivery, the Department stated:

> As required under ERISA section 404, the Department expects that many plan administrators, or their service or investment providers, *already have secure systems in place to protect covered individuals' personal information.* Such systems should reduce covered individuals' exposure to data breaches.[10] (emphasis added)

Although the Department established the new "furnishing" standard, it expressly did not address its intersection with ERISA's fiduciary standards as demonstrated in footnote 35 of the preamble:

> Commenters have asked about the application of ERISA's fiduciary standards and other statutory requirements to electronic disclosure in varying contexts. This safe harbor addresses only a plan administrator's compliance with ERISA's standard for the furnishing of *covered documents to covered individuals.* It neither addresses nor supplants more general fiduciary or other statutory obligations under ERISA. (emphasis added)

---

[8] See 29 CFR § 2520.104b-31(e)(3) and 29 CFR § 2520.104b-31(k)(4)(i).
[9] ERISA Section 404 (a)(1)(B) provides that a fiduciary must discharge his duties with respect to a plan…with the care, skill, prudence and diligence under the circumstances then prevailing that a prudent man acting in like capacity and familiar with such matters would use…"
[10] 29 Fed. Reg. 31916 (May 27, 2020).

Moreover, the Department did not provide guidance as to the expectation, or describe what procedures would be deemed to create "secure systems" and the substantive features of such "secure systems." ERISA's prudent standard of care under Section 404 is an overarching standard, and the Department's statements suggest that plan fiduciaries are subject to the prudent standard of care with respect to PPI, but that there might be some lesser standard in the limited context of electronically furnishing covered documents addressed in the final regulations. While a prudence standard is a higher standard than a reasonableness standard, the different levels of conduct necessary to satisfy each of these standards in any particular circumstance is rarely articulated, which is another reason that additional guidance would be welcome.

We note that many of the covered documents under the 2020 Final Rule, such as participant level-fee disclosures under Department Regulations § 404a-5, are not likely to contain much, if any, PPI. We also question whether the limited additional requirements for disclosures such as quarterly benefit statements, which likely will contain PPI, are adequate protection. Therefore, as a practical matter, the 2020 Final Rule does not provide any clear guidance concerning fiduciaries' obligations under the prudence standard of Section 404 of ERISA.

Department Investigation

Despite not having affirmatively articulated any cybersecurity measures for purposes of meeting the prudence standard of Section 404 of ERISA, the Department, through its Chicago Regional Office of the Employee Benefit Security Administration, has publicly announced its investigation of Abbott Laboratories as plan administrator and Alight Solutions, a plan service provider, to the Abbott Corporate Benefits Stock Retirement Plan "to determine whether any person has violated or is about to violate any provision of Title I of ERISA" with respect to cybersecurity breaches resulting in the loss of assets from participants' accounts. See *Scalia v. Alight Solutions, LLC,* 1:20-cv-02138 (N.D. Il April 6, 2020). This investigation of Title I violations relating to cybersecurity practices (or the lack thereof) also demonstrates the urgent need to clarify the appropriate standards relative to plan administrator measures to protect the cybersecurity of PPI and prevent unauthorized withdrawals from participant accounts.

The lack of clarity from the Department on the application of ERISA Section 404 to protecting PPI is understandable given the rapid pace of technological developments. This guidance is necessary, however, given that such guidance would inform the "circumstances then prevailing" standard under Section 404 against which a plan's cybersecurity protocols would be measured.

Plan fiduciaries, plan administrators, plan service providers, and plan participants are in need of comprehensive guidance with respect to fiduciary responsibility not only in connection with protecting PPI in the electronic furnishing of covered documents, but also for purposes of prudently managing PPI held by the plan and its service providers. Despite the fact that the

Department did not receive substantive comments in response to its cybersecurity question in its 2019 RFI, we urge the Department to move forward on its own initiative to decide what "cybersecurity risk assessments and security measures" can and should be required by regulation.

Therefore, we respectfully request guidance from the Department that addresses the following key questions:

1. What personal information and/or confidential information must be safeguarded by plan administrators and other plan fiduciaries to comply with the fiduciary standards of ERISA Section 404?

2. Is there a difference between plan administrators' overarching duty under Section 404 of ERISA to protect PPI and the "reasonably calculated" furnishing standard in the 2020 Final Rule?

3. For purposes of misappropriation of PPI, is PPI a plan asset under ordinary notions of property rights? Does the resolution of this question affect the application of ERISA's fiduciary standards under Section 404 to protect PPI?

4. What is a plan administrator's responsibility with respect to communicating with participants when there has been an unauthorized appropriation of PPI?

5. What losses due to cybersecurity breaches in the plans' or the plan service providers' systems are covered by a bond under ERISA Section 412 and implementing regulation?

6. What identity verification responsibilities do plan fiduciaries have in instances of accidental loss of PPI and/or accidental failures to follow plan cybersecurity protocols by the participants and beneficiaries?

7. Are state cybersecurity, privacy, and consumer protection laws preempted by ERISA? Are there other state law claims that are not preempted?

1. What personal information and/or confidential information must be safeguarded by plan administrators and other plan fiduciaries to comply with the fiduciary standards of ERISA 404?

While the Department has stated that plan administrators must take action to protect the confidentiality of "personal information," it has not defined the term. Plan administrators, as well as plan service providers, store and transmit participant information (not only for electronic disclosure purposes) and they need clarity as to what information is subject to a fiduciary duty.

2. Is there a difference between plan administrators' overarching duty under Section 404 of ERISA to protect PPI and the "reasonably calculated" furnishing standard in the 2020 Final Rule?

As mentioned above, the 2020 Final Rule requires the plan administrator, or other plan fiduciary, in furnishing required participant disclosures, to take measures *reasonably calculated* to protect the confidentiality of personal information relating to any covered individual. In the preamble, the Department states its assumption that plan administrators, or their service or investment providers, in recognition of the requirements of ERISA Section 404, already have secure systems in place to protect covered individuals' personal information. Plan fiduciaries and their service providers need clarity as to the difference between the two standards.

3. For purposes of misappropriation of PPI, is PPI a plan asset under ordinary notions of property rights? Does the resolution of this question affect the application of ERISA's fiduciary standards under Section 404 to protect PPI?

Currently, it is unclear whether PPI constitutes an asset of the plan. It is one of the questions being litigated in, for instance, a Texas district court in *Harmon v. Shell Oil Co.*, No. 3:20-cv-00021 (S.D. Tex. filed Jan. 24, 2020) (Participants allege PPI is a plan asset and claim fiduciary breach because plan allowed a service provider to use PPI to market nonplan products to participants, allegedly to the participants' detriment.) While the Department has articulated a test as to when an item is a plan asset, the Department has not specifically addressed whether PPI is a plan asset in either advisory opinions or subregulatory guidance. The Department has assumed, in the preamble to the 2020 Final Rule, that protection of PPI is subsumed under the duties of ERISA Section 404, but plan administrators and service providers need confirmation that the 404 duty is not impacted by the unresolved question as to whether PPI is a plan asset. The question of whether PPI is a plan asset may still arise in cases where there is unauthorized appropriation of PPI, but no misappropriation of funds from participants' accounts as of yet. Therefore, guidance on this question would provide additional clarity.

4. What is a plan administrator's responsibility with respect to communicating with participants when there has been an unauthorized appropriation of PPI?

We also request that the Department address the issue of a plan fiduciary's duty to disclose to plan participants when their PPI has been subject to unauthorized access. We recognize that under such circumstances, state laws if applicable, might require disclosure, although such state statutes, to the extent they are not criminal statutes, may be preempted by ERISA at least with respect to the plan itself. We understand that it is the Department's general view that it should not require disclosures beyond those it has required to implement statutes enacted by Congress, but with exceptions.[11] We also believe that the unauthorized access of PPI would be covered by the common law trust principle that a trustee is obligated to disclose to beneficiaries information of which the beneficiary is unaware that a beneficiary needs to protect himself or herself from harm by third parties. A federal court has also concluded similarly,[12] and the Department's subpoena enforcement action in the *Abbott* case, *supra*, indicates a concern that a plan service provider did not notify a participant about a breach. In light of these uncertainties, it is important for the Department to affirmatively articulate a fiduciary standard for such disclosures.

5. What losses due to cybersecurity breaches on plans' or plan service providers' systems are covered by a bond under ERISA Section 412 and implementing regulations?

We request that the Department include guidance on another longstanding concern—the limited scope of ERISA Section 412 (and the Department's implementing regulation) and the advisability of other forms of plan protection. We suspect plan administrators may not fully grasp that the bond required under Section 412 only covers losses caused by fraud or dishonesty by fiduciaries or other plan functionaries that handle plan assets, and may not cover other losses related to cybersecurity breaches. Without a full understanding of the coverage limits, plan fiduciaries will not know to seek other forms of protection for the plan.

In November 2018, the ERISA Advisory Council (the "Council") issued a report to the Department (the "Report") recommending that it update its subregulatory guidance, specifically Field Assistance Bulletin 2008-04, with respect to the bonding requirements under ERISA

---

[11] See generally DOL Request for Information on Disclosures, 65 Federal Register 55858 (September 14, 2000) (solicits comments regarding the extent of an ERISA fiduciary's duty to disclose information to participants and beneficiaries in addition to the specific disclosure requirements imposed under ERISA).

[12] As the Court of Appeals for the Third Circuit stated in *Bixler v. Central Pennsylvania Teamsters Welfare Fund*, 12 F. 3d 1292,1300 (3d Cir. 1993), there is an "affirmative duty to inform when the trustee knows that silence may be harmful." See also Restatement (Second) of Trusts, Section 173, cmt. d (1959) (a trustee "is under a duty to communicate to the beneficiary material facts affecting the interest of the beneficiary which he knows that the beneficiary does not know and which the beneficiary needs to know for his own protection in dealing with a third party.")

Section 412.[13] One recommendation was the addition of a "Fidelity Bond Summary," which would summarize the requirements for securing a fidelity bond that complies with the Department's guidance, to its subregulatory guidance.[14] Such a summary would serve to demystify fidelity bonds for purchasers by explaining the basic requirements, and by helping them to distinguish among the various insurance products that are typically sold in conjunction with 412 fidelity bonds, but that are not subject to statutory mandates under ERISA or the Department's rules and regulations.[15]

While we express no opinion as to whether the Department should implement that recommendation, we believe that it would be appropriate to issue additional subregulatory guidance focusing on the limitations of the Section 412 bond with respect to covered losses, so that plan fiduciaries can better assess what actions may need to be taken to protect participants and beneficiaries against the risk of loss of plan assets as the result of cybercrimes.

6. What identity verification responsibilities do plan fiduciaries have in instances of accidental loss of PPI and accidental failures to follow plan cybersecurity protocols by participants and beneficiaries?

Plan fiduciaries would also welcome guidance as to what responsibilities plan fiduciaries have in situations where participants accidentally lose personal information (*e.g.*, a misplaced driver's license or social security card and/or do not follow plan cybersecurity procedures and educational materials which might include, for example, the danger of exposure of personal information through clicking on suspicious "phishing" emails). We would welcome guidance on what measures can be pursued by plan fiduciaries to ensure compliance with ERISA Section 404 when it does not have control over the protection of PPI outside of the plan.

For instance, is the plan protected by making it explicit in the summary plan description that any person with a participant's user name and PIN is considered the legal participant for purposes of fund withdrawals? In a case where a participant's ex-spouse used the participant's PIN to remove funds from the participant's account, the Court of Appeals held, in a ruling that does not appear limited to domestic situations, that the plan's denial of the participant's subsequent claim for the benefits was not arbitrary or capricious because of the exculpatory summary plan description text. *See, e.g. Foster v. PPB Industries*, 693 F 3rd 1226 (10th Cir. 2012). Although the *Foster* case did not involve any fiduciary breach claims, guidance would be helpful on the extent of the ruling's application under ERISA Section 404.

---

[13] "Evaluating the Department's Regulation and Guidance on ERISA Bonding Requirements and Exploring Reform Considerations," Report to the Honorable R. Alexander Acosta, U.S. Secretary of Labor, Advisory Council on Employee Welfare and Pension Benefit Plans, November 2018.
[14] *Id* at 1 and 8.
[15] *Id* at 8.

7. Are state cybersecurity, privacy, and consumer protection laws preempted by ERISA? Are there other state law claims that are not preempted?

In the event of a cybersecurity breach with respect to PPI, whether unauthorized access to PPI or unauthorized access to participants' accounts, the plan fiduciary could be exposed not only to a claim under ERISA, but also to applicable state law or multiple states laws unless those laws are preempted by ERISA. Plans and/or their service providers may be subject to these types of state law claims in cases such as the *Abbott* case discussed above, involving unauthorized use of PPI to misappropriate funds from a participant's account. Plan fiduciaries would benefit from the Department's view with respect to the parameters under which ERISA preemption of state law claims may apply.

Conclusion

Comprehensive guidance with respect to fiduciary responsibility in this cybersecurity area is needed, not only in connection with protecting PPI when furnishing documents required under Title I of ERISA, but also for purposes of prudently protecting all PPI held by the plan and its service providers. We urge the Department to proceed on its own initiative to determine what cybersecurity risk assessments and security measures can and should be required by regulation.

Thank you for your consideration.

Sincerely,

Marcia S. Wagner

Marcia S. Wagner
Managing Director
The Wagner Law Group

cc: Livia Quan Aber, Esq.
Jordan D. Mamorsky, Esq.
Barry L. Salkin, Esq.
Stephen P. Wilkes, Esq.
(all via e-mail)