THE WAGNER LAW GROUP
A PROFESSIONAL CORPORATION

Stephen P. Wilkes, Of Counsel

EMPLOYEE BENEFITS SECURITY ADMINISTRATION ADVISORY COUNCIL ON EMPLOYEE WELFARE and PENSION BENEFIT PLANS

EXECUTIVE SUMMARY OF WRITTEN TESTIMONY ON CYBERSECURITY May 29, 2015

Good morning. It is a privilege to be here today.

My name is Stephen Wilkes. I am an attorney at The Wagner Law Group, a nationally recognized employee benefits firm, working in our San Francisco office. Our practice encompasses every aspect of employee pension plans ("Pension Plan" or "Plan") and employee welfare plans ("Welfare Plans") as defined under the Employee Retirement Income Security Act of 1974, as amended ("ERISA"), with representation of both plan sponsors and third party product/service providers. We also work with individual retirement account ("IRA") custodians and providers. Because our attorneys draw from many backgrounds including insurance companies and consulting firms, we have the opportunity to consider not only the legal framework but also broader administrative perspectives on many issues.

The ERISA Advisory Council ("Advisory Council") is considering two related topics that each incorporate a "Model Notice" for Pension Plans. Even though I am not a technology consultant or a privacy officer working in the trenches of maintaining and securing a technology platform on a 24/7 basis, our practice has provided me with insight on some larger legal and policy questions that impact the privacy and security of data held by ERISA-covered plans, and IRA's. For purposes of today's discussion, I am using the term "cybersecurity" to include a broad array of issues that may be referred to as privacy, data security, data integrity, data breach, breach notification, etc. I will use Pension Plan or Plan to generally include IRA accounts as well.

I have been asked, today, to discuss some of the legal and policy questions that I have encountered and offer my observations regarding cybersecurity and cybertheft. In other words, what should a Pension Plan sponsor or Pension Plan fiduciary be doing with respect to cybersecurity? What should a non-fiduciary party in interest be doing regarding cybersecurity? Does the identification and implementation of appropriate cybersecurity policy fall within the realm of fiduciary activity under ERISA? Is Plan data a "plan asset" for ERISA purposes? Is there or should there be a role for a Plan participant to play in terms of safeguarding and protecting his or her data?

My presentation will cover: (1) a quick background on some financial service industry and ERISA trends governing information, (2) the status of the cybersecurity regulatory regime in the world of financial services, (3) and raise some policy questions for future consideration by the ERISA Advisory Council.

1. BACKGROUND

I am using financial services as the illustrative backdrop to discuss Pension Plan cybersecurity[1]. Most of the underlying data is financial information (*e.g.*, Plan investments at omnibus and participant level, Plan and participant account balances, account balances held away from the Plan, transaction inflows and outflows, projected benefit levels, projected account balances at retirement, gross and net historical performance data, fees, expenses, etc.) Of course, there is a host of related data that may fall into a different category, such as name and address, age, identification of family and beneficiary, account number, social security number, driver's license number, risk profile metrics, targeted age for retirement, and life expectancy).

Lately, cybersecurity has received a lot of attention. It is not only a topic for professional journals read by financial advisers, lawyers and consultants; it is a recurring headline item every day in major newspapers (such as the data breach of national retailers or health care providers; even the IRS is not immune to cyber attack) and in Congress. The SEC, Financial Institution Regulatory Authority ("FINRA"), Department of Justice ("DOJ"), to name just a few, are agencies or organizations currently engaged in providing public guidance on the topic[2]. Most Americans are attuned at some level to cybersecurity regarding their financial accounts, their personal information, or just the potential reach of the "internet" concerning who you are, what you do, and to potentially take something away. A significant number of people understand the term "hacker", and the phrase "I was hacked".

Many also understand that the risk of theft of personal identity or assets may present itself at any time. This is not a new issue for the Plan world. I would like to acknowledge (and applaud the fact) that the Advisory Council looked at cybersecurity issues four years ago, in the context of maintaining privacy and security around the employee benefit plan platform. It identified identify theft and loss of plan assets as a major concern, caused (potentially) in part by a lack of rigorous cybersecurity policies and procedures in place, and a general failure to appreciate how significant and "real" the cybersecurity threat is to the Pension Plan world. The

---

[1] The subject of cybersecurity in the Welfare Plan world is not discussed today. However, it is noted that although both the Department of Labor ("DOL") and Internal Revenue Service ("IRS") have regulatory jurisdiction on many aspects of health and medical benefit programs, the regulatory regime with respect to cybersecurity of patient information is overseen primarily by the Department of Health and Human Services ("HHS").

[2] *See* for example SIFMA, "Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Businesses" (July 2014); SEC, National Exam Program Alert, "Cybersecurity Examination Sweep Summary" (Feb. 3, 2015), FINRA, "Report on Cybersecurity Practices" (Feb. 2015); Department of Justice, "Best Practices for Victim Response and Reporting of Cyber Incidents", (April 2015)

Advisory Council identified in a practical way different groups, or constituencies, that each had an interest in robust cybersecurity. Those distinct groups may be broken down simply as the Plan sponsor, the participant and beneficiary, and the third party service provider (investment adviser, consultant, third party administrator ("TPA")). The Advisory Council made specific recommendations regarding the fiduciary duty to protect personally identifiable information ("PII"), and the opportunity to provide outreach and education to all of the Plan constituency groups, including retirees. I believe the issues remain very much the same, and that it is timely to reconsider the Advisory Council findings for action by the DOL.

The Pension Plan world is seeking, and relying on, more employee Plan data than ever before. Researchers are collecting and studying this data for various reasons. Financial institutions providing bundled services need this information to control costs and expenses and to improve each participant's "personal experience". Savings and investment rates are used to assess legislative and regulatory positions – consider the implications of the $4.1 trillion retirement savings deficit recently measured by the Employee Benefit Research Institute – and overall retirement readiness. Employers and service providers are interested in the behavioral characteristics of the workforce with regard to savings and productivity. Fiduciary and suitability considerations demand that quantitative metrics such as age, current savings, risk profile characteristics, and account information (both in the Plan and "held-away") be gathered, analyzed, and constantly updated. This data is being transmitted and stored at almost every point of the Plan cycle... starting with the employee/participant and moving to the Human Resource Department of the employer or investment fund office, and then shared and enhanced with the platform provider, trustee, financial adviser and TPA. The technology platform on which these Plan programs reside are becoming more complex, more sophisticated, and more capable than ever. More and more information is being stored in clouds and accessed remotely. The appetite for more and more data is insatiable.

This employee data is at risk both internally and externally. Not only does the Plan sponsor and third party financial service providers have access to this data but other vendors may also have access to this data (*e.g.*, IT providers, data storage companies, etc.)

2. THE LAW

There is no single, comprehensive federal law governing cybersecurity. We are currently working with a complex maze of statutory and regulatory laws at the federal and state level that are not integrated or coordinated. In addition, there are numerous guidelines and suggestions developed by the government and the private sector which are considered "best practices"; these, however, do not have the force of law. The SEC, FINRA, HHS and Federal Trade Commission ("FTC") are active with respect to enforcement at the national level, as are self-regulatory groups such as FINRA - each in its own sphere. The states are very proactive in terms of cybersecurity regulation and enforcement.

Banks, registered investment advisers, registered broker dealers, record keepers, employers, all face one or more sets of legal requirements regarding cybersecurity that touch on Pension Plan matters. Some of the more prominent are as follows:

Gramm-Leach-Bliley Act ("GLB") and Regulation S-P. GLB governs the collection, use and disclosure of financial information. It protects the privacy rights of individuals by limiting how financial institutions may share clients' personal information. It directs that the SEC, as well as other regulators of financial institutions[3], issue rules that implement certain privacy provisions of GLB. Thus, the SEC has issued Regulation S-P for financial institutions over which it has authority (*e.g.*, registered investment advisers[4] and broker dealers). It requires that certain privacy notices be provided to customers and consumers, as well as the opportunity to opt-out and prevent the sharing of certain personal financial information with non-affiliated third parties. It also requires the establishment of procedures reasonably designed to protect client records and information.

It is important to note that Regulation S-P protects individuals, not institutional clients. The SEC has stated that an individual Plan participant is neither a "consumer" nor a "customer" and does not enjoy the protections under Regulation S-P. Pension Plans, structured legally as a "trust", are not "individuals" either. As a result, there may be a significant gap in terms of how Plan data is being protected that needs to be considered. The SEC does note in Regulation S-P that it assumes that under applicable state law, a trustee has its own fiduciary duty to manage the affairs of a trust including the duty to protect beneficiary data, but this should be clarified. State laws may cover individual employers and service providers – but not arising from the fact that they hold Pension Plan data per se.

Regulation S-ID. The Identify Theft Red Flags Rules were adopted jointly by the SEC and the Commodity and Futures Trading Commission. It provides for a set of rules requiring the entities that it regulates to adopt written identify theft prevention polices and procedures that, among other things, implement reasonable policies and procedures to identify, prevent and mitigate the risk of identity theft.

FTCA. FTCA is a federal consumer protection law that prohibits certain trade practices and may be asserted to include cybersecurity activity.

Fair Credit Reporting Act, Fair and Accurate Credit Transactions Act. Federal laws relating to the handling of individual information by consumer reporting agencies.

State Laws. The states have been and remain very active with regard to privacy-related laws and regulations. California and Massachusetts appear to be among the most active and forward thinking in this arena. At my count, forty-seven states have breach notification statutes. Thirty-eight states have social security number protection laws, forty-nine states and the District

---

[3] For example, the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, or FTC.
[4] State-registered investment advisers are regulated by the FTC on privacy matters.

of Columbia have credit report blocking laws, twenty-five states have rules regarding the disposal of personal information, and a handful of states require encryption of customer data. These laws vary state to state, making it a challenge for a business to operate across state lines in a compliant fashion.

We have seen employers, during open enrollment periods when there is a significant exchange of personal data, struggle to comply with the panoply of privacy and security laws if a simple coding or data entry error results in a breach of information (*e.g.*, information is sent to the wrong participant). Determining if a breach occurred in accordance with each applicable federal and state law and complying with each such law is also expensive and can erode plan assets).

3. POLICY QUESTIONS

The policy questions are relatively straightforward. First, is there a gap between the coverage existent under current federal and state law and ERISA with regard to the cybersecurity and integrity of "information" flowing to and from a Plan, Plan participants, and third party service providers? What does that imply? Second, is there/should there be a role for the DOL with regard to Plan cybersecurity? Third, are acts or omissions with regard to cybersecurity a fiduciary function under ERISA? Is it a settlor function? Finally, what interim steps should DOL consider, if any, pending final resolution of the larger policy questions?

Is there a gap? What are the vulnerabilities? The scope and depth of the federal and state laws is actually quite comprehensive. Nonetheless, it is not clear to me whether Plan data (at the participant or the omnibus level) is identified and protected with regard to each and every piece of data transmission, and it may vary state to state as well. I would recommend that the Advisory Council consider that DOL undertake a comprehensive and complete gap analysis to test the integrity of data at both the participant and omnibus Plan level. As part of that process, the DOL may wish to consider whether the current categorization of protected information affords sufficient protection and privacy to participants. For example, Participant A's social security number is generally protected. Participant A's account balance or overall net worth is generally not protected. Should it be protected? The most consequential vulnerabilities may lead to identity theft or loss of plan assets.

DOL Role on Cybersecurity. The Advisory Council's 2011 report is one of the very few, if not the sole authority on the question of the DOL role with regard to Plan cybersecurity. There have been very few commentators, if any, of whom I am aware, speaking on this subject. The Advisory Council provided some well thought out and meaningful suggestions as to how the DOL could step up and speak to cybersecurity in a Plan context. I believe those suggestions remain valid and worthy of consideration, again.

1. Fiduciary status[5]. There is a gating factor to the question of a DOL role in this area, I believe, which must be answered first. Stated simply, there must be clarification around whether the responsibility to address Plan cybersecurity falls within the context of a Plan fiduciary's function (or not). The statute in ERISA Section 3(21)(A) provides in part that a person is a fiduciary to the extent that he exercises discretionary authority or discretionary control respecting management of a plan or exercises any authority or control respecting management or disposition of its assets. It also confers fiduciary status to the extent that a person has any discretionary authority or discretion or responsibility administering an ERISA-covered plan.

Is the Plan sponsor acting as a fiduciary when it establishes a Plan? Or this a settlor function? The courts and the DOL seem to agree that plan adoption, amendment or termination are not fiduciary functions; rather they are settlor functions[6]. Does this mean that when a Plan is adopted, if its design features include a process and procedure for handling Plan and participant data, they are not to be fiduciary decisions? Or is this a discretionary part of administration and management function that is contemplated under ERISA? The law is not clear, and it should be addressed by DOL at some point as a precursor to evaluating how it may otherwise provide guidance to Plan and Plan participants on cybersecurity. In other words, is handling data for cybersecurity something that comes within the meaning of "management" or "administration" as provide under ERISA.

There is a related question, namely, whether Plan data is an "asset" of the Plan over which there may be rendered some form of administration or management.

2. DOL Guidance. Whether Plan cybersecurity is deemed a fiduciary act will drive the structure and format of DOL guidance. If DOL determines that it is not a fiduciary act or responsibility, cybersecurity would be considered a non-fiduciary, purely commercial responsibility of the Plan sponsor. In this case, DOL could still offer guidance to Plan Sponsors regarding the handling of data both at the Plan level and the participant level. Guidance would also need to address the transmission, use and maintenance of data shared with and third party vendors such as financial advisors and record keepers. DOL may also be in a position to identify standard criteria by which Plan sponsors would monitor and select third party vendors with regard to cybersecurity, and perhaps event to identify model representations and warranties contained in a service agreement.

This guidance would likely fall into the category of DOL sanctioned "industry best practices". It is important to note that the evolution of an industry best practice for Plan cybersecurity is already underway. This is likely to become the standard by which someday, I

---

[5] The sole intent of referencing fiduciary status today is to suggest that it is a question requiring some further study. It is respectfully acknowledged that DOL is focused on the fiduciary proposal and related prohibited transaction exemptions at the moment, in the context of investment advice and compensation. It is by no means suggested here that the proposal could have or should have addressed cybersecurity matters.

[6] See DOL Letter (March 13, 1986); Lockheed Corp. v. Spink, 517 U.S. 882 (U.S. Supreme Court, 1996); Hughes Aircraft Co. v. Jacobson, 525 U.S. 432 (U.S. Supreme Court, 1999).

believe, someone will assert that a Plan fiduciary must act with regard to Plan cybersecurity. For example, if the industry standard is to encrypt data upon transmission of the participant files by the Plan sponsor to the recordkeeper, then it would likely be considered a fiduciary breach for the Plan sponsor to transmit unencrypted data because the Plan sponsor must "act with the care, skill, prudence and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims."

CONCLUSION

Thank you for the opportunity to speak and participate on today's panel. The significantly increased flow of Plan and participant data is taking place in an environment where cybersecurity issues abound. The risk of identity theft or loss of plan assets cannot be ignored. Furthermore, the existing overlay of federal and state law may not entirely cover all instances of how data flows in the Pension world. My first suggestion is for DOL to undertake a comprehensive gap analysis to identify weaknesses or holes in the legal system where a person may be unregulated or not required to live up to robust standards concerning cybersecurity issues affecting Pension Plans. Regardless of the gap analysis result, the DOL should ask itself whether it wants to, or should, provide some guidance to Plans on cybersecurity issues. The gating factor here, I believe, is whether the scope and nature of this responsibility at the Plan and/or participant level falls within the definition of a fiduciary under ERISA. I suggest that the DOL provide clarification around this question, as the context of that guidance will differ if it is a fiduciary rather than a non-fiduciary task. Finally, I suggest that the DOL consider providing some guidance in the form of industry best practices.

A0149175.DOC (2)