2-5-2019

Breaches Within Breaches: The Crossroads of ERISA Fiduciary Responsibilities and Data Security

Gregg Moran

Breaches Within Breaches: The Crossroads of ERISA Fiduciary Responsibilities and Data Security

GREGG MORAN*

Although the drafters of the Employee Retirement Income Security Act of 1974 ("ERISA") likely could not have anticipated the data security issues of the twenty-first century, ERISA's duty of prudence almost certainly requires employee benefit plan fiduciaries to protect sensitive participant data in at least some manner. This Article suggests the Department of Labor should issue a regulation clarifying fiduciaries' data security obligations. Given that fiduciaries are in the best positions to recognize their plans' individual security needs and capabilities, the regulation should not attempt to micromanage fiduciaries' substantive data security policies; rather, it should focus on the procedures by which they adopt their substantive policies. In addition to promoting specially tailored policies for protecting sensitive participant data, this regulation would resolve much of the confusion surrounding the application of ERISA to the data security field.

---

* Gregg Moran, attorney in Tampa, Florida. Thank you to my family and friends for their support, particularly my wife, Julianna. Thank you also to the members of the *University of Miami Law Review* for their work editing this piece. Special thanks to Professor Colleen E. Medill. As always, all typos, errors, and bad opinions are my own. The American College of Employee Benefits Counsel selected this Article as the winner of its 2018 Sidney M. Perlstadt Award.

INTRODUCTION

Eighty million people. When hackers gained access to Anthem Insurance's servers, approximately eighty million people could only sit in disbelief, realizing that thieves around the world had access to their private information, including their Social Security numbers.[1] In a sense, a breach of this size can become statistical noise, with commentators focusing on the large-scale implications while ignoring the individual victims.[2] On a different level, however, it is impossible to forget that each of the eighty million line items in the compromised data represents an individual person—an individual person for whom the ever-present menace of identity theft now looms in the background. That reality, in a nutshell, represents the modern data security crisis. Although new technology has granted

---

[1] Shari Rudavsky, *Anthem Data Breach Could Be 'Lifelong Battle' for Customers*, INDYSTAR (Feb. 5, 2015, 7:56 PM), https://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battle-customers/22953623/.

[2] *Cf.* Ronald Bailey, *"The Death of One Man Is a Tragedy, the Death of Millions Is a Statistic."*, REASON: HIT & RUN BLOG (Jan. 7, 2009, 1:32 PM), https://reason.com/blog/2009/01/07/the-death-of-one-man-is-a-trag (suggesting that disasters can start to lose some of their personal impact as they grow in size).

opportunities for society to grow, connecting individuals and data in ways never previously imaginable, it has also opened the door to bad actors who abuse these systems for their own selfish gains. A sophisticated criminal with internet access can now effectively pick the pockets of millions of people worldwide, all from the relative security of a foreign country with lax policing standards.[3]

Confronted with this intimidating and rapidly changing technological landscape, plan fiduciaries under the Employee Retirement Income Security Act of 1974 ("ERISA")[4] often find themselves trying to navigate a minefield without a map. To carry out their basic functions, these fiduciaries must maintain large quantities of highly sensitive participant data.[5] But doing so makes them prime targets for hackers and thieves.[6] Adding to the complexity, these fiduciaries must often give outside service providers (e.g., investment brokers and health insurers) participant data so they can administer ERISA

---

[3] *See* Morgan Chalfant, *Feds Find Some Foreign Hackers Are out of Reach*, HILL (Nov. 29, 2017), https://thehill.com/business-a-lobbying/362458-feds-find-some-foreign-hackers-are-out-of-reach (describing some of the difficulties American law enforcement faces when trying to hold foreign cybercriminals accountable). *See generally Cyber's Most Wanted*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/wanted/cyber (last visited Feb. 21, 2018) (listing the FBI's most-wanted cyber criminals, many of whom hail from foreign countries including Russia, Iran, and China).

[4] Employee Retirement Income Security Act of 1974 (ERISA), Pub. L. No. 93-406, 88 Stat. 829 (codified in scattered sections of 26 and 29 U.S.C.). For purposes of clarity, this Article provides citations to both the ERISA provisions and their corresponding U.S. Code sections. Short-form citations are to the ERISA sections rather than the U.S. Code sections.

[5] *See* Michelle Capezza & August E. Huelle, *Considering Best Data Practices for ERISA Fiduciaries*, LAW360 (May 5, 2015, 1:32 PM), https://www.ebglaw.com/content/uploads/2015/05/Capezza-Huelle-Considering-Best-Data-Practices-For-ERISA-Fiduciaries.pdf (describing challenges and concerns ERISA fiduciaries must manage).

[6] *See id.*

plans.[7] Overlaying this scene is ERISA's duty of prudence, which requires fiduciaries to act "with the care, skill, prudence, and diligence" of a "prudent man" when satisfying their obligations to the plan—a standard that almost certainly requires fiduciaries to safeguard sensitive participant data.[8]

To date, the Department of Labor ("DOL") has been relatively silent with respect to fiduciaries' responsibilities to protect plan data. Aside from the occasional report by the ERISA Advisory Council,[9] fiduciaries lack specific administrative guidance from the DOL regarding issues such as protecting their computers against

---

[7] *See generally* EMP. BENEFITS SEC. ADMIN., U.S. DEP'T LABOR, MEETING YOUR FIDUCIARY RESPONSIBILITIES 1–4 (2017) https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/publications/meeting-your-fiduciary-responsibilities.pdf (providing a basic overview of fiduciary responsibilities when exchanging data with service providers); Norman P. Stein, *I, Fiduciary: Some Reflections on the Definition of Fiduciary Under ERISA*, 6 DREXEL L. REV. 555, 564–55 (2014) (describing broadly how ERISA fiduciaries might transfer some of their administrative or managerial functions to outside service providers).

[8] *See* ERISA § 404(a)(1)(B), 29 U.S.C. § 1104(a)(1)(B) (2012); *infra* Section II.A (applying the duty of prudence in the context of data security).

This Article focuses solely on the theft of *data* from employee benefit plans; it does not address situations in which thieves use stolen data to steal actual plan assets. Simply put, the theft of plan assets poses a different set of issues, given that we can quantify stolen dollars from a pension plan whereas placing a "value" on stolen data is effectively a guessing game. *See infra* Section I.B (addressing the issues of quantifying the harm to consumers resulting from data breaches). To that end, fidelity bonds under ERISA section 412 can address some of the risks posed by insider thefts of plan assets, while commercial crime insurance can address some of the risks posed by outsiders; those options are not as readily available in the data theft context. That said, some of this Article's suggestions—particularly its proposed regulatory emphasis on the *procedures* by which fiduciaries adopt data security plans rather than the *substance* of plans they adopt—could have application in the plan asset context. *Cf. infra* Appendix (outlining a possible regulation the Department of Labor might promulgate to guide plan fiduciaries with respect to their data protection obligations).

[9] *See, e.g.*, ADVISORY COUNCIL ON EMP. WELFARE & PENSION BENEFIT PLANS, CYBERSECURITY CONSIDERATIONS FOR BENEFIT PLANS 1 (2016), https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf [hereinafter 2016 REPORT]; *see also ERISA Advisory Council Reports*, U.S. DEP'T LABOR, https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/erisa-advisory-council/reports (last visited Dec. 15, 2018) (listing reports by the ERISA Advisory Council).

outside attackers and analyzing the data security practices of third-party service providers. Arguably, and somewhat paradoxically, the DOL's past restraint with respect to data security regulation has been the best approach—by not rushing headfirst into the quagmire that is data security, the DOL has avoided some of the criticisms that other regulatory agencies have faced.[10] But continued DOL inaction is no longer appropriate. Rather, DOL action is now critical because ERISA preemption blocks state governments from regulating the data security of employee benefit plans, and no other federal regulatory scheme applies as directly to the issue as ERISA's duty of prudence.[11]

In constructing a regulatory scheme, the DOL has two realistic options. First, it might assume a reactive approach, relying solely on its enforcement authority under ERISA sections 502(a)(2) and 502(a)(5) to shape the duty of prudence's data security requirements through post-breach lawsuits.[12] Second, it might undertake a proactive approach, using its rulemaking authority under ERISA section 505 to give concrete guidance to fiduciaries grappling with data security.[13] This Article argues that the DOL should take a proactive approach. Simply put, quantifying the damages of a data breach is an inexact science at best, meaning that post-breach lawsuits are unlikely to compensate participants or create adequate incentives for fiduciaries to protect data.[14] Although a proactive regulation would

---

[10] *See infra* Section IV.B (describing problems with the reactive regulatory approaches that other agencies, such as the Federal Trade Commission, have adopted).

[11] *See infra* Part III (exploring the regulatory vacuum that exists at both the state and federal levels with respect to the data security practices of employee benefit plans).

[12] ERISA § 502(a)(2), (5).

[13] *Id.* § 505.

[14] *See* David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 937–38 (2016) ("Most of these [data breach damage] cases have failed at the pleading stage. On the consumer side, the problem is that any direct losses usually are reimbursed by the credit card issuer and any potential future losses are speculative.").

still run into this "betrayal without a remedy" situation,[15] it at least would provide the type of guidance fiduciaries need to avoid a breach in the first place, thus making compensation and future deterrence less necessary.

Parts I and II of this Article provide background information, describing the modern data security crisis, the likely application of ERISA's duty of prudence to data security matters, and the DOL's ability to police violations. Part III offers perspective on why continued inactivity by the DOL is inappropriate with respect to data security, given the regulatory vacuum that currently exists in the area. Finally, Part IV proposes a proactive regulatory approach for DOL to adopt that will give fiduciaries substantial guidance with respect to their data security obligations. The full text of the proposed regulation is included as an Appendix.

I. OUR MODERN DATA SECURITY CRISIS

Creating a smarter data security scheme begins with understanding the technological and legal landscape in which businesses operate. In short, ERISA fiduciaries face threats from everywhere—outsiders and insiders alike might steal or otherwise be careless with sensitive data. Fortunately for the DOL, it is not starting from scratch; it can look to the experiences of other agencies and private litigants when designing its regulatory scheme for ERISA fiduciaries. This Part explores the threats modern companies face and the legal system's responses to those threats.

A. *The Threats to Sensitive Data*

All employee benefit plans—retirement and welfare plans alike—require fiduciaries to maintain, use, and share large amounts of sensitive participant data.[16] Although the maintenance of these records, whether in paper or electronic form, allows fiduciaries and

---

[15] Susan Harthill, *The Supreme Court Fills a Gaping Hole:* CIGNA Corp. v. Amara *Clarifies the Scope of Equitable Relief Under ERISA*, 45 J. MARSHALL L. REV. 767, 770 (2012). ERISA literature often uses the phrase "betrayal without a remedy" to describe a situation in which ERISA's remedial scheme under section 502, combined with its broad preemption doctrine, leaves harmed participants unable to recover any damages for a fiduciary's wrongful acts. *See id.* at 770–71; *see also* Allinder v. Inter-City Prods. Corp., 152 F.3d 544, 553 (6th Cir. 1998).

[16] *See* 2016 REPORT, *supra* note 9, at 4–5.

their agents (including third-party service providers) to provide fast, efficient services to plan participants, this convenience comes with risk.[17] Simply put, this information is valuable.[18] Bad actors subject fiduciaries (and other holders of data) to a relentless onslaught of attacks by trying to steal the data for their own purposes.[19] Moreover, these bad actors come from a variety of sources and, although outside attackers represent the most obvious threat to sensitive data, a company's own employees or other insiders also might seek to steal the information.[20]

---

[17] Many publications refer explicitly to "cybersecurity" when discussing modern threats to sensitive data. *See, e.g.*, *id.* But this terminology only encompasses attempts to secure digital data, whereas the term "data security" or "information security" includes attempts to protect both digital and non-digital data. *See* Jackie Buchy, *Cyber Security vs IT Security: Is There a Difference?*, GEO. MASON U. SCH. BUS.: TECH & CYBER BLOG (June 30, 2016), http://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference/. This Article focuses on data security solutions, given that an emphasis purely on cybersecurity would fail to address real-world threats to physical records. *See, e.g.*, J.P. Turner & Co., LLC, Exchange Act Release No. 395, 98 S.E.C. Docket 1729, 2010 WL 2000509, at *4 (ALJ May 19, 2010) (describing a situation in which an employee for an Atlanta-based securities broker left boxes containing thousands of customer records on the street curb outside his home).

[18] *See, e.g.*, Alexandra Ossola, *Why Do Hackers Want Your Health Data?*, POPULAR SCI. (Sept. 10, 2015), https://www.popsci.com/why-do-hackers-want-your-health-data.

[19] *See, e.g.*, Caroline Hummer & Jim Finkle, *Your Medical Record Is Worth More to Hackers than Your Credit Card*, REUTERS (Sept. 24, 2014, 2:25 PM), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (noting an uptick in the number of cyberattacks on health plans); John A. Vogt et al., *Data Breach Risks for 401(k) and Retirement Plans*, JONES DAY (Apr. 2017), https://www.jonesday.com/files/Publication/bf7cbd9d-8bfa-47f1-9417-46f45cbb3bf8/Presentation/PublicationAttachment/6b8622fd-3e6f-48a8-92ca-519e1f3b47ea/Data%20Breach%20Risks%20for%20401(k)%20and%20Retirement%20Plans.pdf (describing an increase in cyberattacks against retirement plans).

[20] *See* PONEMON INST., 2017 COST OF DATA BREACH STUDY 14 (2017), https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/security-ibm-security-services-se-research-report-sel03130wwen-20180122.pdf [hereinafter DATA BREACH COSTS] (finding that "malicious or criminal attacks" are the most common cause of data breaches, including those by employees, contractors, or other insiders).

Further, the motivations driving these attackers vary almost as widely as their identities. For example, private medical data—like a healthcare plan might keep—is surprisingly valuable to criminals who might use it for stealing identities, committing insurance fraud, or even obtaining prescription drugs for resale on the black market.[21] Besides medical records, sensitive plan data can include other items, such as social security numbers, that criminals can use for identity theft.[22] And of course, hackers might obtain lists of passwords and usernames or e-mail accounts that participants use to manage or check on their plan benefits—login information that the participants might reuse for any number of other online accounts.[23]

Compounding the bleakness of this scene is the reality that, at least on some level, data breaches are unavoidable.[24] Data thieves have the time, money, and tools to attack businesses relentlessly—in fact, hackers released around *357 million* new variations of malicious programs in 2016 alone.[25] The most malignant of these programs exploit existing but unknown vulnerabilities in companies' security measures, leaving those seeking to defend against data theft to constantly fight yesterday's battles.[26] Moreover, it seems almost

---

[21] Ossola, *supra* note 18.

[22] *See generally* Hummer & Finkle, *supra* note 19 ("Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number."); Maggie O'Neill, *Hackers Stole More Social Security Numbers than Credit Card Numbers Last Year—Looting $16.8 Billion*, DAILY MAIL (Feb. 22, 2018, 5:13 PM), http://www.dailymail.co.uk/sciencetech/article-5423941/Hackers-stole-Social-Security-numbers-2017.html (describing hackers' attempts to steal social security numbers so they can take funds from the victims' accounts, such as bank and pension accounts).

[23] *See* Ted Samson, *Study Finds High Rate of Password Reuse Among Users*, INFOWORLD (Feb. 10, 2011), https://www.infoworld.com/article/2623504/data-security/study-finds-high-rate-of-password-reuse-among-users.html (describing the prevalence of "password reuse," in which a person uses the same login information for multiple services).

[24] *See* 2016 REPORT, *supra* note 9, at 1 ("Cyber experts say that it is not a question of if you will have a cyber-attack, rather it is a question of when.").

[25] WORLD ECON. FORUM, THE GLOBAL RISKS REPORT 2018, at 14 (13th ed. 2018), www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[26] *See* Dan Goodin, *Zero-Day Attacks Are Meaner, More Rampant than We Ever Thought*, ARS TECHNICA (Oct. 16, 2012, 3:15 PM), https://arstechnica.com/information-technology/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought/ (describing how hackers weaponize undetected vulnerabilities, drawing out cyber-attacks for months or years).

inevitable that sophisticated criminals will someday use advanced artificial intelligence capabilities to steal sensitive records.[27] Under these circumstances, it is no wonder that so many high profile targets have suffered data breaches, including federal agencies such as the State Department, the Internal Revenue Service, and even the National Security Agency.[28] These factors all lead to the inescapable conclusion that the question is not *whether* a business will suffer a breach, but rather *when* the breach will occur.[29]

B. *Legal Responses to the Threats*

Data breaches present somewhat of a legal quandary. Many data breaches clearly involve bad actors: criminals who victimize companies and individuals by stealing sensitive data from them.[30]

---

[27] *See* George Dvorsky, *New Report on Emerging AI Paints a Grim Future*, GIZMODO (Feb. 21, 2018, 1:29 PM), https://gizmodo.com/new-report-on-ai-risks-paints-a-grim-future-1823191087; MILES BRUNDAGE ET AL., THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE: FORECASTING, PREVENTION, AND MITIGATION 21–28 (2018), https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf (describing the potential malicious applications of AI to online data).

[28] *See, e.g.*, Nir Kshetri, *Why the IRS Was Hacked Again and What the Feds Can Do About It*, CONVERSATION (Feb. 16, 2016, 5:50 AM), https://theconversation.com/why-the-irs-was-just-hacked-again-and-what-the-feds-can-do-about-it-54524; Evan Perez & Shimon Prokupecz, *Sources: State Dept. Hack the 'Worst Ever,'* CNN (Mar. 10, 2015, 7:49 AM), https://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html. Although the National Security Agency's most publicized breach came at the hands of Edward Snowden in 2013, it has since faced several other incidents in which insiders stole or attempted to steal highly confidential data. *See* Scott Shane, *Suspect Offers Guilty Plea in Stealing Trove of Secrets*, N.Y. TIMES, Jan. 4, 2018, at A16.

[29] Opderbeck, *supra* note 14, at 936 ("It is not a question of if you will suffer a data breach; it is a question of when."); *see also* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 957 (2016) (quoting a former FBI director as saying, "There are two kinds of big companies in the United States. There are those who've been hacked . . . and those who don't know they've been hacked. . . .").

[30] *See Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes*, TREND MICRO (Aug. 10, 2018), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101 (describing different sorts of data breaches).

An obvious policy goal of any legal system is the desire to hold people accountable for their own actions,[31] which would imply that our focus should be on punishing data thieves and trying to recover their ill-gotten gains. Consequently, the federal government and state governments all outlaw data theft.[32] On the other hand, though, the problem with focusing solely on active wrongdoers in the data security context is that they are often difficult to locate or prosecute, especially when they operate from overseas.[33] More importantly, focusing only on after-the-breach punishment of data thieves does not place enough emphasis on trying to prevent breaches in the first place; the only value it generates in this regard comes in the form of (arguably weak) deterrence.[34] Thus, much of the legal push in the

---

[31] *See generally The Nature of Law*, STAN. ENCYC. OF PHILOSOPHY, https://plato.stanford.edu/entries/lawphil-nature/ (last updated Aug. 7, 2015) (describing the philosophical underpinnings of the legal system and the objective of using law to guide human behavior).

[32] For example, the federal government has the power to prosecute most (if not all, given interstate commerce considerations) data theft involving the use of computers under 18 U.S.C. § 1030 (2012). Additionally, every state has laws prohibiting data theft, including theft via hacking. *See, e.g.*, FLA. STAT. §§ 815.01–815.07 (2018); *see also Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (June 14, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (listing state laws in all fifty states that address hacking, unauthorized access, computer trespass, viruses, and malware).

[33] *See* Roger A. Grimes, *Why It's So Hard to Prosecute Cyber Criminals*, CSO (Dec. 6, 2016, 3:00 AM), https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html.

[34] Legal theory, particularly in the context of criminal law, recognizes two types of deterrence. *See* Brian Jacobs, *The Role of Publicity in Sentencing*, FORBES (Oct. 23, 2017), https://www.forbes.com/sites/insider/2017/10/23/the-role-of-publicity-in-sentencing/#4fb8bd153e5c. General deterrence refers to the expectation that punishing one person will discourage others from engaging in the same behavior. *See id.* Individual deterrence refers to the probability that a punishment will discourage an individual from repeating his or her behavior in the future. *See id.* For purposes of data theft policy, general deterrence is more important, given the number of potential thieves; even if one hacker ceases his or her unlawful activities, another is likely to replace him or her. And while punishing data thieves almost definitely produces at least *some* general deterrence, it is insufficient to deter all such criminals—especially the worst offenders—given the likelihood that they operate outside the effective reach of law enforcement. *See supra* note 3 and accompanying text.

data security realm is on regulating the businesses that keep sensitive data—businesses that are themselves the primary victims in many data breaches.[35]

To be clear, businesses certainly have market incentives to avoid data breaches even in the absence of regulation.[36] Although data breach costs decreased from 2016 to 2017, a recent study of 419 large, global companies revealed average costs of $3.62 million per breach.[37] A company that suffers a data breach can expect to suffer both direct costs, such as the expenses associated with hiring outside forensics experts to analyze the breach, and indirect costs, such as reputational harm and resulting customer loss.[38] A potential issue, however, is that these market incentives often do not sufficiently drive businesses to protect their data; customers bear some of the risk in any breach, meaning the businesses themselves do not face the full costs of data theft.[39] Although this arguably is an appropriate outcome—embodying the idea that everybody should share some of the risk—businesses are undeniably in the best position to prevent data breaches.[40] Therefore, people have tried to use the legal system, through both private lawsuits and direct regulation, to push the full costs of data breaches onto the companies that suffer them, which may in turn incentivize those companies to take additional precautions.[41]

---

[35] *See, e.g.*, FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016).

[36] *See* DATA BREACH COSTS, *supra* note 20, at 5–7 (discussing the average costs of data breaches to companies).

[37] *Id.* at 1.

[38] *Id.* at 29.

[39] Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1508, 1519–21 (2013).

[40] *Id.* at 1517–18 (describing the economics view that the law should allocate risks to low-cost avoiders—i.e., those who are in the best positions to mitigate or avoid risks).

[41] *See generally id.* at 1533–35 (discussing the challenges of applying traditional tort law to cybersecurity issues); Elaine F. Harwell, *No Signs of Slowing Down: Privacy Litigation Update*, FOR DEF., Oct. 10, 2017, at 91, 93, https://www.selmanlaw.com/sites/default/files/FTD-1710-Harwell.pdf (noting that major data breaches are the likely cause of an increase in privacy litigation and regulatory enforcement actions).

To date, attempts to shift data breach costs onto businesses via private litigation have been limited because of the difficulties associated with quantifying and tracing the harms of breaches.[42] Plaintiffs who try to recover from companies in the aftermath of data breaches face a number of legal hurdles, each of which has the potential to derail their claims. For starters, circuits are split over whether individuals suffer a sufficiently concrete injury and therefore have standing to sue a business that suffered a breach when the individual's sole injury is the mere loss of data resulting from the breach.[43] Even if an individual plaintiff survives the standing requirement, he or she is hardly ensured a victory.[44] First, the plaintiff in a standard negligence case must prove the defendant was negligent in how it handled the sensitive data.[45] Second, a plaintiff in any data breach litigation is going to have issues showing causation, given that he or she might have also lost his or her data in any number of other breaches of unrelated companies or sources, including

---

[42] *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739–46 (2018) (discussing difficulties courts face in conceptualizing harms posed by data breaches and how those difficulties lead to limited redress for plaintiffs).

[43] *See* Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017) (listing the circuit courts that have analyzed the issue, along with their holdings). The Sixth, Seventh, Ninth, and D.C. Circuits have found that an increased risk of future identity theft is sufficient to confer standing, while the First, Third, and Fourth Circuits have rejected that position. *Id.* Note that *Beck* does not cite to the D.C. Circuit's decision finding standing, because the D.C. Circuit issued its opinion six months after the Fourth Circuit issued *Beck*. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017).

[44] Although the number of data breaches has grown alarmingly with time, the litigation framework for these cases remains underdeveloped, given that the cases that survive the standing requirement tend to settle. *See* Harwell, *supra* note 41, at 93.

[45] *See* Resnick v. AvMed, Inc., 693 F.3d 1317, 1325–26 (11th Cir. 2012) (listing negligence claim elements and addressing sufficiency of the pleadings in a data security context).

yet-undiscovered breaches.[46] Third, some courts have used a theory known as the economic loss doctrine to bar plaintiffs' tort claims, given that their claims arise "solely in economic damages unaccompanied by physical or property damage."[47] In short, being a data breach victim is miserable, but being a data breach victim trying to sue the company that lost the data is even worse.

In contrast, governmental agencies that regulate businesses' data security practices can avoid many of the traps that afflict private litigants, such as the need to show a concrete injury-in-fact stemming from a data breach.[48] At the federal level, "the most prominent regulatory agency" to address data security is the Federal Trade Commission ("FTC").[49] The FTC's strategy has been to bring enforcement actions against companies that suffer breaches using its authority to regulate "unfair . . . acts or practices,"[50] under the theory that lax data security practices are unfair to customers.[51] Of course, the FTC is not the only federal entity that seeks to regulate data security; other governmental bodies also regulate this area and take varying

---

[46] *See id.* at 1327; Harwell, *supra* note 41, at 93. Notably, issues relating to causation and damages might also prevent class certification, given that Rule 23(b)(3) requires common questions of law or fact to predominate over individual matters. *See, e.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 293 F.R.D. 21, 30, 33–34 (D. Me. 2013) (denying class certification in a data breach case because the plaintiffs did not produce expert testimony regarding the *total damages* the proposed class allegedly suffered). It is unlikely individual plaintiffs would pursue their claims in the absence of a class, given the relatively low dollar amounts at stake per person in a data breach.

[47] Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F. 3d 162, 175 (3d Cir. 2008) (quoting Adams v. Copper Beach Townhome Cmtys., L.P., 816 A.2d 301, 305 (Pa. Super. Ct. 2003)). A fuller description of the economic loss doctrine is well beyond the scope of this Article; it is enough to know that it poses another hurdle to prospective data breach plaintiffs. *See generally* Opderbeck, *supra* note 14, at 944–46.

[48] *See e.g.*, Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, FLA. B.J., July/Aug. 2016, at 30, 38 (citing R.T. Jones Capital Equities Mgmt., Exchange Act Release No. 4204, 2015 WL 5560846 (Sept. 22, 2015)) (discussing how the SEC brought an enforcement action even though the hacked company's clients suffered no actual economic harm).

[49] Hooker & Pill, *supra* note 48, at 38.

[50] 15 U.S.C. § 45(a) (2012).

[51] *See id.*; Hurwitz, *supra* note 29, at 964–66.

approaches to the issue. For example, the Department of Health and Human Services governs the data security practices of health plans and providers by means of a complex set of regulations under the Health Insurance Portability and Accountability Act ("HIPAA").[52]

Likewise, state legislatures regulate data security, with every single state having passed breach notification laws that require businesses and government agencies to inform the public about security breaches involving private customer data.[53] State administrative agencies are also beginning to play a role in the data security realm—for example, the New York State Department of Financial Services recently promulgated strict regulations imposing numerous data security requirements on financial institutions, such as mandating they designate Chief Information Security Officers.[54] In short, while other government agencies like the FTC have attempted to regulate data security, the DOL has not, thereby leaving a regulatory void with respect to the security of data in employee benefit plans.[55]

II. ERISA'S FIDUCIARY STRUCTURE

ERISA's fiduciary obligations are the heart of its regulatory scheme.[56] ERISA designates persons holding trusted positions in the administration of an employee benefit plan as fiduciaries,[57] requir-

---

[52] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). The security and privacy regulations under HIPAA are available at 45 C.F.R. §§ 160, 164(a), (e) (2018).

[53] *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES, (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[54] N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.0–500.23 (2018).

[55] *See infra* Part III. Though beyond the scope of this Article, companies operating abroad also face regulation by foreign governments, such as the European Union. *See, e.g.*, Daniel K. Alvarez, *The EU General Data Protection Regulation Is Coming—Is Your Client Ready?*, PRAC. LAW., Oct. 2017, at 19; Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2017).

[56] *See* Employee Retirement Income Security Act of 1974 (ERISA) § 2(b), 29 U.S.C. § 1001(b) (2012) ("It is hereby declared to be the policy of [ERISA] to protect . . . the interests of participants in employee benefit plans and their beneficiaries . . . by establishing standards of conduct, responsibility, and obligation for fiduciaries of employee benefit plans . . . .").

[57] *See id.* §§ 3(16), (21)(A), (38), 402(a)(1).

ing them to follow certain standards when performing their obligations to the plan.[58] Ultimately, one of these duties—the duty of prudence—forms the basis for concluding that fiduciaries *must* take steps to protect sensitive plan data. Section II.A explores the duty of prudence both generally and in the context of data security, and Section II.B addresses the DOL's authority to enforce the provisions of ERISA, including its ability to assess fines for noncompliance.

A. *The Duty of Prudence*

ERISA's duty of prudence is paramount in the context of data security.[59] It requires fiduciaries to carry out their obligations to the plan "with the care, skill, prudence, and diligence under the circumstances" that a prudent man "familiar with such matters" would utilize.[60] Importantly, prudence does not require a good outcome; a fiduciary might behave prudently even if he or she does something that ends badly.[61] A good illustration of this principle arises in the context of underperforming investments in pension plans: federal

---

[58] *See id.* §§ 404–06.

[59] Three other obligations might have at least some relevance to the data security issue. First, the exclusive benefit rule almost certainly prohibits fiduciaries from selling participant data or using it for purposes other than providing benefits. *See id.* § 404(a)(1)(A). Second, fiduciary might face liability if it knows of a cofiduciary's failure to safeguard plan data but does nothing to remedy the situation. *See id.* § 405(a)(3). Third, fiduciaries must comply with plan provisions expressly relating to data security, provided doing so is prudent. *See id.* § 404(a)(1)(D); Herman v. NationsBank Tr. Co., 126 F.3d 1354, 1358 (11th Cir. 1997).

[60] ERISA § 404(a)(1)(B).

[61] *See, e.g.*, Tatum v. RJR Pension Inv. Comm., 761 F.3d 346, 369 (4th Cir. 2014) (explaining that the duty of prudence does not impose liability on fiduciaries who use "reasoned decision-making process[es]," even if their decisions "yield outcome[s] that in hindsight prove . . . less than 'optimal'"); Bd. of Tr. of City of Birmingham Emps.' Ret. Sys. v. Comerica Bank, 767 F. Supp. 2d 793, 802 (E.D. Mich. 2011) ("The ultimate outcome of an investment is not proof of imprudence.").

courts routinely affirm that the decision-making process, as opposed to the outcome of a particular investment, determines prudence.[62]

Another relevant component of the duty of prudence is the duty to monitor third parties that provide services to the plan. This duty to monitor relies on the idea that fiduciaries can—and do—delegate plan administrative tasks to various service providers. But, in any principal-agent relationship, a prudent principal will take ongoing steps to ensure the agent performs his or her duties with care.[63] These steps include assessing potential agents before ever hiring them,[64] as well as continually reviewing their post-hiring work.[65] Thus, ERISA fiduciaries who seek to act prudently must take similar steps with respect to the third-party service providers they hire as agents, even if those service providers are not themselves fiduciaries.[66]

Although nothing in ERISA expressly defines the protection of sensitive data as a "dut[y] with respect to a plan"[67] and no case law

---

[62] As the District of Hawaii explained:

> Virtually every investment entails some degree of risk, and even the most carefully evaluated investments can fail while unpromising investments may succeed. The application of ERISA's prudence standard does not depend upon the ultimate outcome of an investment, but upon the prudence of the fiduciaries under the circumstances prevailing when they make their decision and in light of the alternatives available to them.

Marshall v. Glass/Metal Ass'n & Glaziers & Glassworkers Pension Plan, 507 F. Supp. 378, 384 (D. Haw. 1980).

[63] *See, e.g.*, EMP. BENEFITS SEC. ADMIN., DEP'T OF LABOR, FIELD ASSISTANCE BULLETIN NO. 2015–02 (2015); *see also* Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 308 (1976) (describing the monitoring, bonding, and residual costs that principals incur to control their agents).

[64] *See, e.g.*, Donovan v. Mazzola, 716 F.2d 1226, 1233–34 (9th Cir. 1983).

[65] *Cf.* Tibble v. Edison Int'l, 135 S. Ct. 1823, 1827–29 (2015) (holding that an ongoing failure to remove imprudent investment choices from a plan menu tolled the relevant statute of limitations under ERISA); Colleen Medill, *Regulating ERISA Fiduciary Outsourcing*, 102 IOWA L. REV. 505, 520–21 (2017) (making the point that ERISA should be interpreted to require fiduciaries to monitor co-fiduciaries to whom they outsource their duties).

[66] Ellen Mondress, *Contracting Tips of ERISA Plans*, BENEFITS MAG., May 2012, at 39.

[67] Employee Retirement Income Security Act of 1974 (ERISA) § 404(a)(1), 29 U.S.C. § 1104(a)(1) (2012).

addresses the issue, ERISA's duty of prudence almost certainly requires fiduciaries to attempt to guard plan data.[68] Simply put, a fiduciary *cannot* operate an employee benefit plan modernly without collecting and using participant data. Pension plans must have access to account information, health plans must have access to medical records, and all plans must have access to information that identifies individual participants.[69] No reasonable person "familiar with such matters" would ever consider *not* taking any steps to protect sensitive data.[70] And, along these same lines, the duty must require fiduciaries to inspect the data security practices of third-party service providers they hire because no reasonable person would entrust somebody to work with sensitive data without first determining that he or she will try to keep it safe.[71] In short, the question is not *whether* the duty of prudence requires the protection of plan data, but rather *how* fiduciaries can comply with the obligation.[72]

---

[68] A few unreported opinions have analyzed data breaches involving ERISA plans, but none has analyzed the duty of prudence. *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-02633, 2017 WL 539578 (D. Or. Feb. 9, 2017); Anthem, Inc. Data Breach Litig., No. 15–MD–02617–LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016). The DOL's 2016 report does not expressly say the duty of prudence entails a requirement to protect sensitive data, but it at least hints at the issue by using the word "prudent" three times. *See* 2016 REPORT, *supra* note 9 at 5, 23.

[69] *See* 2016 REPORT, *supra* note 9, at 7–8 (describing information retained by benefits plan providers).

[70] *See* ERISA § 404(a)(1)(B).

[71] *See* Ariel Gaknoki, *Cybersecurity and ERISA: Fiduciary Obligations to Safeguard Plan Participants' Data*, TRUCKER HUSS 1, 2 (June 2017), https://www.truckerhuss.com/wp-content/uploads/2017/06/2017-06_fid_ob_data.pdf ("[T]he Bulletin has been interpreted more broadly to establish the requirement of prudence in service provider selections, including prudence in the selection of a service provider that maintains electronic plan data in order to keep that plan data private and secure.").

[72] *See generally id.* Undoubtedly, some future litigant will try to argue that ERISA does not obligate fiduciaries to protect plan data. But surely ERISA must involve *some* duty to protect data the fiduciary uses while operating the plan; concluding otherwise would seemingly lead to the absurd result that a fiduciary could purposefully make private information publicly available without violating ERISA's duty to act as a reasonable person when carrying out plan duties. *Id.*

B. *The DOL's Enforcement Role*

ERISA's fiduciary duties are meaningless without a working enforcement mechanism. Although the DOL, Internal Revenue Service, Department of Justice, and private litigants all play a role in enforcing ERISA,[73] participant lawsuits and DOL actions serve as the primary means of ensuring fiduciary compliance.[74] Within its role as the primary regulatory agency charged with enforcing ERISA, the DOL can take both proactive and reactive enforcement actions. On the proactive side of the equation, the DOL has rulemaking authority to prescribe any regulation it finds "necessary or appropriate" to fulfill ERISA's purposes.[75] As part of this authority, the DOL can regulate the plan-related books and records fiduciaries maintain, which certainly could permit it to require fiduciaries to create records relating to their data security practices.[76]

On the reactive side of the DOL's authority, it can bring actions against fiduciaries and other parties that violate ERISA's provisions and the DOL's own regulations.[77] The problem with this enforcement power, however, is that the DOL likely cannot prove damages by, or recover adequate damages from, a fiduciary that acts imprudently with respect to data security.[78] As with private litigants demonstrating standing in data breach lawsuits,[79] the problem the DOL faces in seeking monetary recovery against a fiduciary with poor data security practices is measuring concrete harm—courts

---

[73] *See* Dana M. Muir, *Decentralized Enforcement to Combat Financial Wrongdoing in Pensions: What Types of Watchdogs Are Necessary to Keep the Foxes out of the Henhouse?*, 53 AM. BUS. L.J. 33, 68 (2016).

[74] *See* ERISA §§ 2(b), 502(a)(1)–(3), (5).

[75] *Id.* § 505.

[76] *Id.*

[77] *See id.* § 502.

[78] *See* Solove & Citron, *supra* note 42, at 737 (discussing the difficulty of quantifying monetary harms from a data breach).

[79] *See generally supra* notes 45–49 and accompanying text.

have struggled, and will likely continue to struggle, with quantifying the damages that consumers suffer as a result of data breaches.[80]

This inability to impose monetary damages—itself an example of a "betrayal without a remedy" under ERISA's labyrinthian remedial framework—limits the DOL's ability to push the costs of a data breach onto the offending fiduciaries, reducing some of the incentives those fiduciaries otherwise might have to scrutinize and improve their own data security practices.[81] Even civil and criminal penalties under ERISA have limited potential to apply in data breach scenarios. First, civil penalties by the DOL are entirely off the table. The DOL can only assess an amount equal to twenty percent of the amount recoverable as damages in an action,[82] and twenty percent of $0 is still only $0. Second, although criminal penalties for data breaches can be indeterminate amounts not tied to quantifiable and

---

[80] *See generally* Solove & Citron, *supra* note 42, at 737 (discussing the struggles of courts to quantify the harms associated with data breaches, finding many of these struggles arise "from the fact that data-breach harms are intangible, risk-oriented, and diffuse"). In their article, Professors Solove and Citron propose that courts ought to be more willing to quantify the harms resulting from data breaches, especially in light of the fact that courts quantify intangible types of harm in many other contexts. *Id.* at 746. Although courts *might* adopt this type of thinking in the future, it would require a dramatic change of course from their usual approach to data breach litigation. *See id.* at 785. And beyond the desire to maintain consistency with past opinions, courts might have practical reasons for wanting to avoid recognizing damages arising from data breaches—for example, recognizing the ability to recover damages might also encourage strike suits. *See id.* at 782.

[81] Harthill, *supra* note 15, at 770–71 (discussing the problems that arise when ERISA preempts state laws but leaves harmed participants without any ability to recover damages, known as a *betrayal without a remedy*); *see supra* notes 38–42 and accompanying text (discussing how legal damages can incentivize companies to better consider the harms that might result from their lax data security practices—i.e., causing them to internalize the externalities they might otherwise create).

[82] Employee Retirement Income Security Act of 1974 (ERISA), § 502(l)(1)–(2), 29 U.S.C. § 1132(l)(1)–(2) (2012).

recoverable damages, only the Department of Justice can seek these penalties.[83]

In short, the DOL—the main regulatory agency tasked with enforcing ERISA—has *no* ability to impose monetary costs on fiduciaries with lax data security practices. None of this is to conclude that DOL enforcement actions should not play any role with respect to regulating employee benefit plans providers' data security practices. The DOL can always pursue equitable remedies, such as asking a court to remove a fiduciary that does not adequately protect participant data.[84] But, the point is to recognize the limits the DOL would face under the current statutory scheme if it were to adopt a purely reactive approach to regulation.[85] If the DOL hopes to have any impact on the data security practices of ERISA fiduciaries, it needs to adopt a proactive approach that gives fiduciaries concrete guidance they can use to develop and assess their policies and procedures.

---

[83] *See id.* § 501(a). The other problem with relying on criminal fines to serve as a major deterrent to inadequate data security practices is that the Department of Justice must show the breach of prudence was willful, which would require a showing the fiduciary purposefully had lax data security. *See id.*; *cf.* United States v. Phillips, 19 F.3d 1565, 1576, 1584 (11th Cir. 1994) (requiring fiduciaries to "voluntarily, knowingly, and intentionally" engage in conduct for section 501 to apply). Beyond the burden of making a willfulness showing, it seems unwise to conclude the Department of Justice would have any ability or interest in becoming the chief regulator of employee benefit plans' data security practices, a conclusion supported by the fact that Westlaw, as of January 20, 2019, reports only 199 opinions even involving section 501.

[84] ERISA § 409(a).

[85] Congress could always resolve this problem by giving the DOL the ability to issue fines not tied to recoverable damages, much like the Department of Justice can do in criminal actions, at least with respect to situations (like data breaches) in which damages are non-quantifiable. For example, Congress could set a statutory cap (either on a per-occurrence or per-participant basis) and then give the DOL flexibility to determine appropriate fines based on the severity of the fiduciary's misconduct. That said, there is no reason to expect Congress will act on the matter; this Article focuses solely on regulatory changes the DOL can make without Congressional action.

III. THE IMPORTANCE OF ERISA TO DATA SECURITY POLICY

To date, surprisingly little case law addresses ERISA's potential significance in the area of data security.[86] This Part argues, however, that ERISA is more than just generally applicable to data security matters. In fact, it is vitally important given its unique applicability to employee benefit plans. As a result, the DOL must assume a stronger role in regulating fiduciaries' data security practices. Section III.A explores the possibility of ERISA preempting state laws that attempt to govern data privacy and security. Section III.B describes the lack of any other federal regulations governing employee benefit plans, leaving the DOL with the responsibility of addressing this void.

A. *ERISA Preemption of State Laws*

ERISA's broad preemption doctrine removes authority to regulate employee benefits plans from the states and puts it in the hands of the federal government.[87] Though ERISA's statutory preemption rule is relatively brief, preempting state laws that "relate to any employee benefit plan,"[88] the Supreme Court has repeatedly expanded on its meaning in high-profile cases, including its most recent venture into the area: *Gobeille v. Liberty Mutual Insurance Co.*[89] In brief, ERISA preempts two categories of state laws.[90] The first category consists of any state law that acts "immediately and exclusively upon ERISA plans" or that requires the existence of an ERISA plan for its operation.[91] The second category includes state

---

[86] Daniel O'Neil, *Employee Benefit Plans and Data Security Issues*, JACKSON LEWIS (Apr. 25, 2016), https://www.benefitslawadvisor.com/2016/04/articles/fiduciaryduties/employee-benefit-plans-and-data-security-issues/ (noting that scope of ERISA in area of data security remains uncertain, as it has yet to be addressed by courts).

[87] ERISA § 514(a).

[88] *Id.*

[89] 136 S. Ct. 936, 943 (2016).

[90] *Id.*

[91] *Id.* (quoting Cal. Div. of Labor Standards Enf't v. Dillingham Constr., N.A., 519 U.S. 316, 325 (1997)).

laws that impermissibly govern "central matter[s] of plan administration" or "interfere[] with nationally uniform plan administration."[92]

Applying these standards, the second category of ERISA preemption seems to cover most—if not all—state law claims, statutes, and regulations purporting to govern the data security practices of employee benefit plans.[93] First, ERISA likely preempts tort claims against plan fiduciaries in the aftermath of data breaches. As described before in Section II.A, the duty of prudence almost certainly requires fiduciaries to take at least some steps to protect plan data. A negligence claim against a plan fiduciary in the aftermath of a breach would effectively allege that the fiduciary was negligent in performing his or her duty to protect plan data, which is exactly the type of state-law claim to which ERISA's preemption rule should apply.[94] Therefore, these state-law tort claims infringe upon central matters of plan administration—i.e., the standards by which we judge fiduciaries' conduct.[95]

Likewise, ERISA arguably preempts the various breach notification laws that states have enacted as laws that interfere with nationally uniform plan administration. For example, if an employee benefit plan has participants in fifteen states, it might have to provide fifteen different types of notifications in the aftermath of a data breach affecting the plan.[96] Moreover, the *Gobeille* Court emphasized ERISA's "extensive" reporting, disclosure, and recordkeeping requirements, finding that compliance with these obligations is a

---

[92] *Id.* (quoting Egelhoff v. Egelhoff *ex rel*. Breiner, 532 U.S. 141, 148 (2001)).

[93] In contrast, the first category of ERISA preemption likely would not apply to any existing state data security laws, given that none of them purports to rely upon or apply exclusively to employee benefit plans. *See id.* at 945.

[94] *Cf.* Corcoran v. United HealthCare, Inc., 965 F.2d 1321, 1331 (5th Cir. 1992) (holding that ERISA preempted a medical negligence claim against a claims reviewer that denied a treatment, resulting in the death of the plan participant's unborn child).

[95] This result becomes even more likely if the DOL adopts regulations for the protection of plan data, given that the state laws might conflict with the DOL's own directives.

[96] *See* Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, A.B.A: LAW TECH TODAY (Apr. 19, 2016), https://www.lawtechnologytoday.org/2016/04/crazy-quilt-work-state-data-breach-notification-laws-just-got-crazier/.

central matter of plan administration.[97] Accordingly, state laws requiring disclosure of certain events to plan participants seem to intrude upon the authority of Congress and the DOL to regulate the disclosures that plans must make.[98] Given the likely preemption of tort claims and breach notification laws, it seems highly probable that ERISA would further preempt any state laws or regulations that purport to govern with particularity the means by which plans must protect their data, such as those promulgated by the New York State Department of Financial Services.[99]

Whether ERISA preemption of state-level data security laws is a beneficial result is debatable. Although it would create uniform national standards for employee benefit plans, it would simultaneously undercut states' abilities to serve as "laboratories of democracy"[100] by trying new and innovative approaches to data security

---

[97] *Gobeille*, 136 S. Ct. at 944.

[98] *Cf. id.* at 945–46 (holding that ERISA preempted a Vermont law requiring healthcare plans to send reports about healthcare costs to a state agency).

[99] *See generally* N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.0–500.23 (2018). For an example of how the New York regulations would intrude upon the administration of an employee benefits plan, consider the requirement under section 500.04 that every covered entity install a "Chief Information Security Officer" ("CISO") in charge of overseeing implementation of the regulations. *Id.* § 500.04. In essence, a CISO would become a "functional fiduciary" under ERISA section 3(21) by having "discretionary authority . . . in the administration" of the plan's data protection strategy. *Id.*; Employee Retirement Income Security Act of 1974 (ERISA) § 3(21), 29 U.S.C. § 1002(21) (2012). Thus, the New York regulations purport to tell covered employee benefit plans to install specific fiduciaries not required by ERISA's own terms.

[100] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

regulation.[101] Regardless, ERISA preemption in this context certainly would be an impactful result.[102] The preemption of state-level laws leaves a regulatory vacuum because existing ERISA remedies are likely inadequate, both in terms of relief offered to injured plan participants and deterrence of lax data security practices by fiduciaries.[103] Consequently, there is a pressing need for the DOL to develop standards in the area through proactive regulation.

B. *The Federal Regulatory Desert*

Although ERISA preempts state laws purporting to govern the conduct of fiduciaries, it does not excuse fiduciaries from their obligations under other federal laws.[104] Nevertheless, no existing federal statutes or regulations compare to ERISA in terms of ability to govern the data security standards of employee benefit plans. For example, one of the most well-known federal laws relating to data security is the Gramm–Leach–Bliley Act ("GLBA"), which applies

---

[101] *See generally* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 923, 927–31 (2009) (outlining the risks associated with federal preemption of state experimentation).

[102] To be sure, it is not a foregone conclusion that the Supreme Court would find ERISA preempts all state-level data security laws—the Supreme Court's preemption jurisprudence has evolved over time, and it has not always been consistent with past opinions. *See generally* Edward A. Zelinsky, *ERISA Preemption After* Gobeille v. Liberty Mutual*: Completing the Retrenchment of* Shaw, 34 HOFSTRA LAB. & EMP. L.J. 301, 303–11 (2017).

[103] *See supra* Section II.B (explaining the problems with quantifying damages resulting from a data breach).

Given the potentially far-reaching effects of ERISA preemption, it is even more surprising that very little case law even considers its application. Only two cases explore in any real depth the possibility of ERISA preempting state laws applying to data security, and neither does so in a convincing manner—both ignore the duty of prudence and its possible consequences to the analysis. *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-02633, 2017 WL 539578, at *1, *16–20 (D. Or. Feb. 9, 2017); *In re* Anthem, Inc. Data Breach Litig., No. 15–MD–02617–LHK, 2016 WL 3029783, at *39–50 (N.D. Cal. May 27, 2016). Both of these cases analyzed express plan language promising to guard plan data, determining whether those contractual promises were recoverable "benefits" available under the plan. *See In re Premera*, 2017 WL 539578, at *18; *In re Anthem*, 2016 WL 3029783, at *43–44. Moreover, there is a lack of academic literature in the area, probably caused by the fact that data law as a field is relatively young, and both data law and ERISA are specialty practice areas.

[104] Employee Retirement Income Security Act of 1974 (ERISA) § 514(d), 29 U.S.C. § 1144(d) (2012).

to various actors in the financial industry.[105] By its own terms, however, the GLBA only applies to nonpublic *consumer* information.[106] Even if employees who participate in pension plans sponsored by covered entities arguably fit within the statutory definition of "consumer,"[107] the regulatory agencies tasked with rulemaking under the GLBA tend to exempt participants in employee benefit plans.[108] And, in any case, the GLBA does not apply to businesses outside the financial industry, such as health insurers or administrative service providers.[109]

Likewise, HIPAA is also not a good substitute for regulating the data security practices of employee benefit plans. To be clear, healthcare plans are covered entities subject to the data privacy regulations under HIPAA.[110] But that means HIPAA governs only a subset of all employee benefit plans; it completely ignores pension plans and many types of welfare benefit plans. Moreover, HIPAA

---

[105] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (2012) (codified in scattered sections of 12 and 15 U.S.C.).

[106] *See, e.g.*, 15 U.S.C. § 6801(b) (2012) (requiring specific regulatory agencies to adopt standards for protecting "customer records and information"); *see also* 17 C.F.R. § 248.30 (2018) (requiring certain types of investment intermediaries to protect "customer records and information"). The GLBA seems to use the terms *customer* and *consumer* interchangeably, though most references in the statutory provisions are to consumers.

[107] *See* 15 U.S.C. § 6809(9) ("The term 'consumer' means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes . . . .").

[108] *See* 17 C.F.R. § 248.3(g)(2)(viii) ("An individual is not your [customer] solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary."); *see also* 16 C.F.R. § 313.3(e)(2)(viii) (2018) (providing an identical rule for the financial companies expressly subject to the Federal Trade Commission's authority under the GLBA).

Notably, the GLBA and its implementing regulations require covered third-party providers of financial services to guard plan data they receive from pension plans. *See supra* note 106. So even though the GLBA might not *expressly* apply to the plans themselves, the ERISA Advisory Council was incorrect in its 2016 report when it implied that existing federal laws do not require actors within the financial industry to protect sensitive pension data. *See* 2016 REPORT, *supra* note 9, at 7 (finding that the GLBA does "not apply directly to . . . the sensitive individual data held in conjunction with [benefit] plans").

[109] *See generally* 15 U.S.C. § 6809(3) (defining "financial institution").

[110] 45 C.F.R. §§ 160.102–160.103 (2018).

does not require covered entities to monitor third-party service providers,[111] meaning it has less reach than ERISA does.[112]

Finally, the FTC might try to assert its status as the "most prominent" data security agency by using its expansive "unfair . . . acts or practices" authority to regulate the data security efforts of ERISA plans.[113] This, however, would be an unsatisfactory outcome. First, the FTC's approach is entirely reactive because it is based on post-breach lawsuits, which in turn limits its value with respect to guiding regulated entities.[114] Second, the FTC might not have jurisdiction to govern participants in employee benefit plans—its "unfair practices" authority only extends to actions that can harm "consumers,"[115] and its Enabling Act does not define which people are consumers.[116] Third, and most importantly, the FTC has no particular expertise in working with plan fiduciaries or analyzing ERISA documents. In sum, other federal agencies are ill-equipped to address the problem of data breaches involving employee benefit plans. The

---

[111] *See id.* §§ 160.102–160.103, 164.504(e); *Is a Covered Entity Liable for, or Required to Monitor, the Actions of Its Business Associates?*, DEP'T HEALTH & HUMAN SERVS. (Dec. 19, 2002), https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html.

[112] As an aside, application of HIPAA to a healthcare plan leads to somewhat of a preemption paradox. Because HIPAA is a federal law, fiduciaries of healthcare plans must comply with it. Employee Retirement Income Security Act of 1974 (ERISA) § 514(d), 29 U.S.C. § 1144(d) (2012). But while HIPAA itself preempts some state laws governing data security and privacy, it expressly excludes others from its preemption rules, including laws that are "more stringent" than the requirements under HIPAA. *See* 42 U.S.C. §§ 1320d-2, 1320d-7 (2012); 45 C.F.R. §§ 160.202, 160.203(b). At face value, HIPAA should not affect ERISA preemption of those state laws, because it only exempts them from *HIPAA* preemption and does not purport to say anything about *ERISA* preemption. The counterargument, however, is that by exempting certain "stringent" state laws from preemption, HIPAA essentially requires covered entities to comply with them, which in turn arguably makes compliance with those state laws a "law of the United States" not subject to ERISA preemption. *See* ERISA § 514(d). The answer here *seems* to be that ERISA preempts state laws even if HIPAA does not, given that HIPAA does not affirmatively *impose* those state laws. That said, the ultimate solution to this riddle is beyond the scope of this Article.

[113] *See* 15 U.S.C. § 45(a), (n).

[114] *See infra* Section IV.B (explaining the guidance failures that reactive regulatory approaches create in data law).

[115] *See* 15 U.S.C. § 45(n).

[116] *See id.* § 44.

DOL remains the go-to agency for matters affecting employee benefit plans and must use its expertise to provide guidance for fiduciaries and protection for participants.[117]

IV. A PROPOSED APPROACH TO THE DUTY OF PRUDENCE AND DATA SECURITY

Although the DOL needs to assume a role in governing the data security practices of employee benefit plans, it first must have a coherent plan for how it intends to do so. Section IV.A summarizes the underlying policy goals the DOL should strive to achieve. Section IV.B explores why purely reactive regulatory approaches—i.e., post-breach lawsuits—do not provide the type of meaningful guidance that is necessary in a rapidly changing and technologically involved field such as data security. Section IV.C outlines the substantive language the DOL can use in its regulation, and Section IV.D explains how the proposed regulation, which appears as an Appendix to this Article, satisfies the DOL's policy goals.

A. *Policy Goals of Data Security Regulation*

Stating that the goal of a data security law is to "protect data" seems needlessly vague and redundant, but laws in the field often take that exact approach.[118] This Article proposes that any good data security law will consider three separate, concrete policy objectives.

---

[117] *See, e.g.*, *Health Plans & Benefits*, U.S. DEP'T LABOR, https://www.dol.gov/general/topic/health-plans (last visited Dec. 15, 2018) (describing the DOL's oversight of health plans and benefits); *Retirement Plans-Benefits & Savings*, U.S. DEP'T LABOR, https://www.dol.gov/general/topic/retirement (last visited Dec. 15, 2018) (describing the DOL's oversight of employee benefits); *Fiduciary Education Campaign*, U.S. DEP'T LABOR, https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/fiduciary-responsibilities/fiduciary-education-campaign (last visited Dec. 15, 2018) (describing the DOL's Fiduciary Education Campaign, which provides tools for ERISA fiduciaries to build "an understanding of the law and their responsibilities"); *Field Assistance Bulletins*, U.S. DEP'T LABOR, https://www.dol.gov/agencies/ebsa/employers-and-advisers/guidance/field-assistance-bulletins (last visited Dec. 15, 2018) (listing Field Assistance Bulletins, which offer guidance to providers).

[118] *See, e.g.*, 15 U.S.C. § 6801 (describing the purpose of the GLBA as "respect[ing] the privacy of . . . customers and . . . protect[ing] the security and confidentiality of . . . nonpublic personal information").

First, it will try to minimize the number and severity of breaches by encouraging companies to adopt suitable defenses. Second, it will try to help victims of breaches recover. And third, it will try to minimize costs for regulated entities. Fortunately for the DOL, these three goals should look very familiar—they are analogous to ERISA's goals of deterring fiduciary misconduct,[119] protecting plan participants' interests,[120] and not imposing unnecessary administrative costs on the sponsors of employee benefit plans.[121]

The first goal—minimizing the number and severity of breaches—involves encouraging companies to adopt suitable defenses against data breaches through a mix of deterrence and guidance. Data security laws seek to establish at least some definite requirements for regulated entities,[122] impose costs on regulated entities that fail to meet those requirements, and educate regulated entities about their obligations.[123] Importantly, data security experts across the board agree that individual companies *must* have the flexibility to design their own practices for protecting sensitive data

---

[119] *Cf.* Employee Retirement Income Security Act of 1974 (ERISA) §§ 409, 501–02, 29 U.S.C. §§ 1109, 1131–32 (2012).

[120] *Cf. id.* § 502(a)(1)(B) (permitting participants or beneficiaries to recover their promised benefits through private lawsuits).

[121] *See* Mertens v. Hewitt Assocs., 508 U.S. 248, 262–63 (1993).

[122] Often, however, these "definite requirements" are only unclear standards, such as a requirement that companies "reasonably design[]" their defenses. *See* 17 C.F.R. § 248.30(a) (2018).

[123] Administrative agencies routinely provide guidance about data security—particularly cybersecurity—to regulated entities. *See, e.g.*, 2016 REPORT, *supra* note 9. The best example of administrative guidance is the National Institute of Standards and Technology's voluntary framework for critical infrastructure. *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2017), https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf [hereinafter NIST FRAMEWORK].

based upon their unique needs and capabilities.[124] The alternative approach, in which a law imposes a laundry list of necessary data security policies and procedures, would undermine the goal of protecting sensitive data by diverting attention to "wooden compliance with a checklist of practices that may reduce future *liability risk*, but do not advance enterprise *security*."[125] Moreover, the practical issues with trying to impose a top-down list of requirements are insurmountable. Even if a governmental entity could come up with a perfect list of data security practices that would apply equally well to all regulated entities (an impossible task), it would have trouble keeping that list current with rapid changes to technology and threats.[126]

Unlike the first goal, which focuses on avoiding breaches or at least limiting their severity, the second goal emphasizes helping people in the breaches that will inevitably occur. In other words, it requires asking, "What can we give to the people who lost their sensitive data in the breach and now are probably at an increased risk of identity theft?" To date, answering this question has befuddled the legal system. The most logical way to compensate victims of any type of harm is through private lawsuits and the common law of torts, but plaintiffs in data breach cases routinely fail to demonstrate

---

[124] *See, e.g.*, Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2259 (2015) [hereinafter *Scope and Potential*] ("[D]ata security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist."); Luis A. Aguilar, Comm'r Sec. & Exch. Comm'n, A Threefold Cord - Working Together to Meet the Pervasive Challenge of Cyber-Crime, Speech at the SINET Innovation Summit (June 25, 2015), https://www.sec.gov/news/speech/threefold-cord-challenge-of-cyber-crime.html ("[E]ntities must develop procedures that are tailored to their unique risks. This is essential, as it avoids a check-the-box approach to cybersecurity . . . .").

[125] Archis A. Parasharami & Stephen Lilley, Wyndham*, Heartbleed, and the Pitfalls of Setting Cybersecurity Standards Through Litigation*, COMPUTER L. REP., June & July 2014, at 22, 27 (2014) (emphasis added); *see, e.g.*, *Scope and Potential*, *supra* note 124, at 2259; Aguilar, *supra* note 124.

[126] *See generally* Thomas O. McGarity, *Some Thoughts on "DeOssifying" the Rulemaking Process*, 41 DUKE L.J. 1385, 1385–86 (1992) (describing the amount of time it takes a federal agency to pass a regulation under the Administrative Procedure Act).

concrete injuries for standing purposes, much less prove actual damages.[127] Of course, money is not the only thing a law could provide to a data breach victim; breach notification laws seek to provide victims with information about data breaches, presumably reminding those victims to take steps to protect themselves (e.g., checking their credit scores).[128] And even if a law does not require it, companies that experience breaches might have reputational reasons to offer free credit monitoring services to their customers.[129]

Finally, the third goal of any good data security policy is cost control—regulations that impose too great of costs will inevitably stifle innovation and cause society greater harm than a data breach ever would.[130] Similar to its ERISA counterpart, however, this goal

---

[127] *See supra* Section I.B; Opderbeck, *supra* note 14, at 937–38 (describing the common types of plaintiffs in data breach lawsuits and the difficulties they have encountered). Even if a statute purported to give victims a defined cash amount in the aftermath of a breach (e.g., $50 per breach), those victims would still have to demonstrate standing in any private lawsuit to enforce the statute. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545, 1547–48, 1550 (2016) (holding that a plaintiff in a Fair Credit Reporting Act ("FCRA") lawsuit still had to prove the defendant's violation actually caused him to suffer a concrete injury even though the FCRA provided a defined recovery amount of $100 to $1000 per willful violation).

[128] *See* Dennis Fisher, *Data Breach Disclosure Laws Don't Work*, COMPUTER WKLY. (June 10, 2008, 5:00 AM), https://www.computerweekly.com/news/2240022032/Data-breach-disclosure-laws-dont-work ("[N]otification laws do one thing very well: notify consumers of a data breach.").

[129] *See* PONEMON INST., THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT 1 (2014), https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf [hereinafter DATA BREACH AFTERMATH].

[130] *Cf.* COMM. FOR ECON. DEV., CONFERENCE BD., REGULATION & THE ECONOMY: THE RELATIONSHIP & HOW TO IMPROVE IT 3–4 (2017), https://www.ced.org/pdf/CED_Report-Regulation_and_the_Economy2.pdf (quoting ORG. ECON. COOPERATION DEV., REGULATORY POLICY AND GOVERNANCE: SUPPORTING ECONOMIC GROWTH AND SERVING THE PUBLIC INTEREST (2011)) ("Regulations can also have unintended costs, when they become outdated or inconsistent with the achievement of policy objectives. The 2008 financial crisis—which resulted in part from poorly designed regulatory regimes and the uneven enforcement of existing regulations—and the ensuing and ongoing economic downturn starkly illustrate the potential consequences of regulatory failure.").

For example, a theoretical way to prevent most data breach risks would be to outlaw companies from storing *any* sensitive data in electronic format. But people and companies probably would not be pleased with a law like this, given that it would eliminate many of our modern capabilities and comforts.

takes a secondary role to the other priorities. At face value, this policy objective normally seems to conflict with the first two goals; a dollar more of deterrence or victim compensation is a dollar less of savings. But a creative data security law will find a way to minimize this conflict, especially given that businesses themselves stand to lose sizeable amounts of money if they are victims of data breaches.[131]

In practice, every law that seeks to regulate data security must strike a balance between these often-competing goals, seeking to maximize each while acknowledging that some sacrifices are necessary. That said, regulatory entities should not focus solely on the theoretical justifications for their laws; they must consider whether their laws provide the desired results in practice.[132] For example, consider breach notification laws. These laws generally seem to emphasize the first two goals (deterrence and compensation) while mostly ignoring the cost-control objective, except to the extent that they might impose lesser costs than some alternatives. Their success on the first two objectives, however, is suspect at best—experts disagree about whether they impose great enough costs on businesses to deter poor security practices,[133] and the value of the notifications to victims is equally unclear.[134] Nevertheless, these three policy

---

[131] DATA BREACH COSTS, *supra* note 20, at 1 (discussing the average costs of data breaches). In other words, if the costs of suffering a breach outweigh the costs of defending against the breach, then the company would actually save money by implementing the protections.

[132] COMM. FOR ECON. DEV., *supra* note 130, at 3.

[133] *See* Marcus Ranum & Bruce Schneier, *State Breach Notification Laws: Have They Helped?*, TECHTARGET (Jan. 10, 2009), https://searchsecurity.techtarget.com/magazineContent/State-Data-Breach-Notification-Laws-Have-They-Helped?vgnextfmt=print (debating the value of breach notification laws); *cf.* DATA BREACH AFTERMATH, *supra* note 129, at 1–10, 14–22 (studying the effects that breach notifications have on business-consumer relationships).

[134] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5565, 5642 (Jan. 25, 2013) (finding that too many notifications might cause breach victims "unnecessary anxiety or even eventual apathy"); Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 280–81 (2011) (suggesting that many victims who receive breach notifications do not take steps to protect themselves).

goals provide a framework for analyzing the intended and likely effects of any proposed data security law.

B. *Reactive vs. Proactive Regulatory Approaches*

Before advancing to this Article's proactive regulation, it is worth revisiting the alternative: a reactive approach under which the DOL uses post-breach enforcement actions to provide guidance on a case-by-case basis. In addition to the problem already addressed in Section I.B—the difficulty in quantifying data breach harm—the reactive regulatory approach would not adequately guide fiduciaries in their substantive responsibilities.[135] At best, a post-breach enforcement action can only hope to capture a historical understanding of a data security practice based on a certain set of facts, explaining why a specific defendant either lived up to or fell short of the enforcing agency's standards.

Proponents of administrative rulemaking-through-adjudication dispute this point, arguing that agency actions can build "the functional equivalent of common law" for data security purposes.[136] For example, Professors Solove and Hartzog created a list of twenty-five "inadequate security practices" as derived from the FTC's civil actions against companies.[137] But again, this list of practices was only current as of 2014 when they wrote their article, and we can only be certain of how these principles applied to *specific* companies that suffered *specific* data breaches.[138] Moreover, some of these listed "principles" are so broad as to be effectively useless to companies trying to plan data security practices, such as the suggestion that those companies could face punishments for "failure[s] to monitor data recipients' activit[ies]."[139]

Ironically, the amorphous nature of a reactive regulatory approach is actually one of its features—proponents argue that it enables administrative agencies to avoid the normal difficulties associated with drafting comprehensive regulations that are sufficiently

---

[135] *See supra* notes 126–30 and accompanying text (describing the importance of guidance as a goal).

[136] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2014) [hereinafter *Common Law of Privacy*].

[137] *Id.* at 651–55.

[138] *See generally id.*

[139] *Id.* at 654.

broad without creating too many unintended secondary effects.[140] But this reactive approach would raise serious hindsight bias concerns. A fiduciary might use every possible defense but still suffer a data breach; the risk is that a factfinder might give too much weight to the mere occurrence of the breach when considering whether the fiduciary did enough.[141] Moreover, the idea that businesses must look to a collection of quasi-case law to determine their legal responsibilities is troubling, especially considering the legal expenses it would impose on small companies that might want to do nothing more than establish benefit plans for their employees.[142]

Finally, the best-case scenario for this reactive approach, as far as guidance to regulated entities is concerned, is that experts in the field could synthesize the agency's opinions into a list of compliance requirements.[143] Again, however, these lists would only be historical records in a rapidly evolving field, and they would risk incentivizing regulated entities to engage in unwanted checkbox compliance that actually undermines data protection.[144] In short, a purely reactive regulatory approach would be undesirable even if the DOL could issue fines—it would impose needless uncertainty and costs on fiduciaries trying to follow the DOL's actions, and it would place an emphasis on judging yesterday's problems rather than addressing tomorrow's threats.[145]

C. *The Substance of the Duty to Protect Data*

The DOL's task in creating a data security regulation might sound nearly impossible. Its final product needs to carefully balance

---

[140] *See Scope and Potential*, *supra* note 124, at 2264–65.

[141] *Cf.* Maggie Wittlin, *Hindsight Evidence*, 116 COLUM. L. REV. 1323, 1359–62 (2016) (describing the issues that hindsight bias can create for a factfinder in a lawsuit). Of course, the mere occurrence of a breach is not proof of imprudence. Even the National Security Agency has suffered multiple breaches. *See* Shane, *supra* note 28.

[142] *See* Mertens v. Hewitt Assocs., 508 U.S. 248, 262–63 (1993); Hurwitz, *supra* note 29, at 1012.

[143] *Cf. Common Law of Privacy*, *supra* note 136, at 619, 651–55 (compiling a list of principles from FTC cases and touting them as being the "the functional equivalent of common law").

[144] *See supra* note 129 and accompanying text.

[145] *See* Parasharami & Lilley, *supra* note 125, at 23.

the goals of encouraging fiduciaries to craft their own suitable defenses, protecting the interests of plan participants, and avoiding the creation of unnecessary cost barriers.[146] Likewise, the final product must be clear enough that it will be useful in guiding fiduciaries' behavior even considering the DOL's statutory inability to impose monetary penalties.[147] At the same time, however, the regulation cannot go too far in prescribing substantive defensive measures, such that fiduciaries fall into the trap of checkbox compliance by focusing more on meeting the DOL's particular (and non-tailored) requirements than meeting their own unique needs.[148] Finally, the DOL's regulation must maintain its relevance even as technology and new threats continue to evolve at whirlwind paces.[149]

Fortunately, the DOL can meet these objectives by taking a fresh approach to data security regulation that builds upon the duty of prudence's application in other contexts. To date, every governmental entity that has tried to regulate data security has focused on the *substance* of the policies and procedures that regulated entities develop, even if by stating only that the policies and procedures must be "reasonabl[e]."[150] Rather than adopting this old approach, the DOL should focus instead on the *procedures* by which fiduciaries develop their data security practices. In other words, the duty of prudence's

---

[146] *See generally supra* Section IV.A.

[147] Although ERISA's remedial scheme in its current form will inescapably hobble some of the DOL's enforcement ability in the data security context, *see supra* Section II.B, a sufficiently clear regulation can hopefully overcome some of the deterrence losses through the forcefulness with which it defines fiduciaries' obligations.

[148] *See, e.g.*, Parasharami & Lilley, *supra* note 125, at 23.

[149] *See generally* CISCO, ANNUAL CYBERSECURITY REPORT 3–4 (2018), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf (describing developing cybersecurity threats, including self-propagating malware and the challenges of adapting cybersecurity to new areas such as new internet-connected devices and cloud platforms).

[150] *See, e.g.*, 17 C.F.R. § 248.30(a) (2018). Even breach notification laws take this approach, requiring regulated companies to adopt certain substantive policies and procedures (e.g., notify consumers in the aftermath of data breaches). *See Security Breach Notification Laws*, *supra* note 53.

application to data security must mirror its application to floundering pension investments—care in decision-making, rather than substantive outcomes, must determine prudence.[151]

The best way to accomplish this outcome is by promulgating a regulation that conveys three messages to fiduciaries.[152] The first of these messages must be that the fiduciaries themselves have broad discretion to design and adopt data security policies and procedures that meet their own needs and abilities.[153] In this way, the DOL would actually give creative control to the fiduciaries, thus following the expert consensus that optimal data security results from regulated entities being able to tailor-make their own policies and procedures to meet their unique situations.[154]

The DOL's regulation must clarify this overarching freedom with its second message to fiduciaries—they must act honestly when considering, adopting, and implementing their data security practices.[155] After all, the only way a self-created policy or procedure will have value in protecting sensitive data is if the fiduciary genuinely seeks to achieve the goal of data protection when designing it and acts prudently in doing so. At first glance, this focus on what we might call good-faith efforts seems to replace one uncertain standard ("were the fiduciary's ultimate data security practices substantively prudent?") with another ("did the fiduciary adopt its ultimate data

---

[151] *Cf.* Bd. of Tr. of City of Birmingham Emp.'s Ret. Sys. v. Comerica Bank, 767 F. Supp. 2d 793, 802 (E.D. Mich. 2011) ("The ultimate outcome of an investment is not proof of imprudence.").

[152] The Appendix provides draft language of a regulation the DOL could promulgate at 29 C.F.R. § 2550.404a-6 (currently unused). To explore how the specific regulatory language incorporates the concepts described above, this Section will cite directly to the Appendix, using provisions of the proposed regulation as though it were an existing regulation.

[153] *See infra* Appendix, at (b)(1)(ii), (c)(1)(i).

[154] *See generally* NIST FRAMEWORK, *supra* note 123, at 2 ("[This] Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can priorities investments to maximize the impact of each dollar spent.").

[155] *See infra* Appendix, at (a)(4), (b)(1)(i)–(ii), (c)(1)(i), (f)(2).

security practices in a prudent manner?").[156] But the DOL can overcome this potential issue with the regulation's third crucial message: fiduciaries have the burden of *affirmatively proving* they acted prudently in considering data security policies and procedures, and they must *keep detailed records as evidence* of that prudence.[157]

To be effective, these records must contain enough information so that the DOL can assess whether a fiduciary approached its data security obligations with the actual focus of protecting participant data.[158] Fortunately, by placing the burden on fiduciaries to prove they acted prudently, the regulation actually incentivizes them to create and maintain these records; every record a fiduciary can produce of a policy or procedure it considered is another piece of evidence it can use to bolster its case.[159] Notably, the regulation should distinguish between records the fiduciary keeps with respect to its own policies and procedures and those it makes when selecting and monitoring third-party service providers.[160] This distinction flows from the fact that a fiduciary will have different considerations when protecting data in its possession than when it ensures outsiders are also protecting the data.[161]

One added bonus of the regulation's emphasis on procedures and recordkeeping requirements is that it gives some teeth to the DOL's role as an enforcer.[162] Although it might not be obvious at first, one of the implications of requiring fiduciaries to consider policies and procedures that might protect their data is that the DOL itself has the power to suggest substantive practices they might adopt. The DOL might do this broadly, such as by issuing a guidance letter with respect to a new technology, or it might do it individually after auditing a particular plan's data security policies. This DOL power to offer suggestions does not change the fact that the fiduciary has the ultimate discretion to decide whether to adopt or reject the

---

156 *See infra* Appendix, at (a)(1)–(5).

157 *See infra* Appendix, at (b)(3)–(4), (c)(2)–(3), (e).

158 *See infra* Appendix, at (a)(1)–(5).

159 *See infra* Appendix, at (b)(3).

160 *Compare infra* Appendix, at (b) (the fiduciary's policies and procedures for protecting data that it keeps), *with* Appendix, at (c) (third-party service provider selection).

161 *See supra* note 160.

162 *See supra* Section II.B.

proposal.[163] But if the fiduciary does not at least consider the proposal and create a record of its decision-making process, it will effectively prove it was not acting with the goal of protecting its data.[164]

Beyond those three primary messages, the regulation must cover a few other technical matters. First, in addition to providing fiduciaries the freedom to *adopt* their own policies and procedures, the regulation must expressly recognize their ability to *reject* considered policies in good faith, even if DOL regulators might have recommended its adoption.[165] Otherwise, the fiduciaries will not actually have the ability to design their own policies and procedures in any meaningful sense. Second, the regulation should prescribe at least a few substantive policies and procedures that fiduciaries must adopt—they must have plans for keeping all their policies and procedures current, vetting potential service providers, and monitoring existing service providers.[166] Third, the regulation should encourage cost control by permitting multiple fiduciaries for a plan to keep only a single set of records, rather than trying to maintain them on a per-

---

[163] *See infra* Appendix, at (f)(2).

[164] *See infra* Appendix, at (e)(1)(ii) (requiring fiduciaries to prove they sought to protect data). Paragraph (e)(2) of the regulation provides factors for making this analysis. These factors seek merely to provide helpful guidance, rather than a conclusive element test, for analyzing a fiduciary's good-faith compliance.

[165] *See infra* Appendix, at (f)(2).

[166] *See infra* Appendix, at (b)(2). Notably, the DOL must still give fiduciaries the flexibility to shape their particular plans described in this paragraph. But the point is that every plan should have some version of these three substantive policies, given their universal applicability. For example, all plans must keep their policies and procedures current, and it is consistent with the rest of the regulation to provide the fiduciaries themselves the freedom to decide *how* they will keep the policies and procedures current.

fiduciary basis.[167] Fourth, the regulation should generally have precise wording, considering that its value as a source of guidance to fiduciaries will naturally flow from its clarity.[168]

D. *Policy Benefits of the Proposed Regulation*

Simply put, this proposed focus on procedure over substance fits well with the policy goals of data security regulation.[169] It certainly advances the objective of minimizing the number and severity of data breaches by providing fiduciaries with clear obligations while still respecting their unique needs and capabilities.[170] At the same time, it avoids the risks of checkbox compliance by refusing to prescribe substantive requirements other than recordkeeping obligations and a few minor limitations on fiduciary discretion as described above.[171] Finally, it is designed to withstand the tests of time and the evolution of technology. The best substantive practices for

---

[167] *See infra* Appendix, at (d).

[168] A fifth consideration that might appear in the regulation would be to clarify whether plan participants and beneficiaries may request these records. Plan participants and beneficiaries can demand copies of "instruments under which the plan is . . . operated," which *might* arguably include any policies or procedures for securing plan data. Employee Retirement Income Security Act of 1974 (ERISA) § 104(b)(4), 29 U.S.C. § 1024(b)(4) (2012). Alternatively, we might view those records as being standard human resources policies for safeguarding employee information, rather than substantive documents governing the administration of benefits in line with the plan's overarching purpose. But the release of any records showing the plan's data security practices might compromise those practices, which benefits neither the plan itself nor the participants that ERISA is designed to protect. Of course, this potential issue likely already exists in the absence of any regulation for sophisticated fiduciaries who already maintain policies and procedures for safeguarding plan data. Nevertheless, the DOL's regulation might expressly exempt data security policies from disclosure under a section 104(b)(4) request, or it might permit fiduciaries to redact the documents, only provide a summary of the documents, or only produce a list of the documents. *See generally Id.* § 505 (granting the DOL broad authority to issue regulations under ERISA).

[169] *See supra* Section IV.A. It also recognizes that *nobody* has all the answers with respect to protecting data. *Id.*

[170] *See supra* Section IV.A.

[171] *See supra* Section IV.C.

protecting data constantly change; the procedures by which thoughtful companies consider and adopt those practices, however, remain constant.[172]

Moreover, it advances the cost-control outcome in a couple of ways. First, the freedom it provides fiduciaries permits them to operate within their own means. Second, and somewhat indirectly, it promotes good data security practices, which in turn reduces complying fiduciaries' risks of suffering data breaches and incurring the related economic costs.[173] As a result, it would avoid being needlessly burdensome on fiduciaries and employers that sponsor employee benefit plans.

Most importantly, the proposed regulation provides needed clarity in a developing and constantly shifting area of the law.[174] It instructs fiduciaries and the attorneys who advise them while simultaneously assuring participants of what they can expect from the people and businesses entrusted with their data. Otherwise, an indeterminate term like "prudence" might take on any number of meanings in the data security context—it could imply a focus on the substantive policies fiduciaries adopt, the procedures by which they adopt them, or some mix of the two.

Under the Supreme Court's *Hardt v. Reliance Standard Insurance Company* decision, a plaintiff can win an award of attorney

---

[172] The proposed regulation does not expressly purport to advance the second goal of data law—compensating breach victims—in any concrete way. Given the historical challenges that this policy outcome has posed for the legal system, it seems most appropriate to afford fiduciaries the same flexibility in determining the best ways to care for their participants who lose data in a breach. And it is not outside the realm of possibility to assume they might actually do a fine job of this. Companies have economic incentives to "compensate" their consumers who suffer data losses—e.g., by offering free credit monitoring services. *See, e.g.*, Christine DiGangi, *Anthem Breach Victims Can Get Free Credit Monitoring This Week*, YAHOO FIN. (Feb. 12, 2015), https://finance.yahoo.com/news/anthem-breach-victims-free-cedit-180017134.html.

[173] *See* DATA BREACH COSTS, *supra* note 20, at 26–28 (analyzing the costs that businesses experience in the aftermath of data breaches).

[174] *See* Hooker & Pill, *supra* note 48, at 31 (describing the current state of cybersecurity law as a "legal fracas" requiring attorneys to utilize "a patchwork of common law and state or federal statutory claims to obtain relief").

fees merely by showing "some degree of success on the merits" regardless of whether he or she ultimately wins damages.[175] As a result, fiduciaries are almost certain to face lawsuits even without DOL action in the area of data security.[176] But DOL guidance would help plaintiffs focus their efforts on fiduciaries that actually do engage in misconduct by not considering data security practices or keeping appropriate records, and it would help responsible fiduciaries ward off frivolous lawsuits quickly and efficiently. Everybody would benefit from increased clarity regarding data security practices, and the DOL has all the tools it needs to provide that necessary guidance.[177]

CONCLUSION

Although the DOL has not yet provided ERISA fiduciaries concrete guidance on the duty of prudence's application to data security, it is in a perfect position to do so. Armed with the benefit of academic works and other agencies' experiences, it can craft the duty of prudence in a manner that encourages the protection of sensitive data while remaining consistent with other applications of the duty.

---

[175] 560 U.S. 242, 255 (2010) (citing Ruckelshaus v. Sierra Club, 463 U.S. 680, 694 (1983)).

[176] Any lawsuits would need to be under ERISA section 502(a)(3) or 502(a)(5), which permit the DOL, plan participants, beneficiaries, or fiduciaries to petition for "appropriate equitable relief" to address ERISA violations, including duty-of-prudence breaches. Employee Retirement Income Security Act of 1974 (ERISA) § 502(a), 29 U.S.C. § 1132(a) (2012). Although ERISA section 502(a)(2) permits damages lawsuits (as opposed to equitable ones) against ERISA fiduciaries who breach their duties, the recoverable damages in those cases must go to the plan itself; individual participants and beneficiaries cannot recover compensatory or punitive damages. Mass. Mut. Life Ins. Co. v. Russell, 473 U.S. 134, 144–48 (1985). As a result, participants cannot attempt to use ERISA section 502(a)(2) to attempt to claim damages resulting from any breach, such as the costs of purchasing identity protection plans. But even though an award of "appropriate equitable relief" under ERISA section 502(a)(3)—such as an order to cease acting imprudently with respect to data security—would not entitle participants to money damages, victorious plaintiffs could (and likely would) still recover attorney fees. ERISA § 502(g)(1). Therefore, the incentive to bring post-breach lawsuits against fiduciaries remains.

[177] Even in the absence of an affirmative regulation from the DOL, the standards described in the draft regulation, located in the Appendix of this Article, likely are best practices. The point is that the DOL's formal adoption of a regulation would carry with it a sense of authority.

The DOL's goal is straightforward: encourage the creation of flexible, inventive, and tailored plans for addressing the modern threat of data theft. By emphasizing the procedures by which fiduciaries develop their data security practices, rather than the substantive practices themselves, the DOL can promote a new system that encourages responsibility, flexibility, and—above all else—security.

APPENDIX

PROPOSED LANGUAGE OF THE NEW REGULATION

29 C.F.R. § 2550.404a-6: Fiduciary Requirements for the Protection of Sensitive Data.[178]

(a) **In General.**

(1) The duty of prudence found in section 404(a)(1)(B) of the Employee Retirement Income Security Act of 1974, 29 U.S.C. § 1104(a)(1)(B), requires fiduciaries of employee benefit plans to protect the sensitive data they encounter during the course of their duties.

(2) Complying with the duty of prudence with respect to protecting sensitive data involves both securing any sensitive data the fiduciary keeps in its possession, as well as vetting and monitoring service providers who have access to any sensitive data.

(3) A fiduciary must comply with this section to meet the requirement to protect sensitive data under the duty of prudence.

(4) The purpose of this section is to encourage fiduciaries to consider and develop their own data security policies and procedures with the honest goal of protecting sensitive data, given that fiduciaries are in the best position to analyze the plan's individual needs and capabilities in this regard.

(5) This section shall only apply to persons acting in their capacities as fiduciaries.

---

178 *Cf.* Gregg Moran, *The SEC's Data Dilemma*, 96 NEB. L. REV. 446, 482–83 (2017) (applying similar concepts to the Security and Exchange Commission's Safeguards Rule of 17 C.F.R. § 248.30).

(b) **Duty with Respect to Data in the Fiduciary's Possession or Control.**

(1) **Requirements.**

(i) The fiduciary must consider and adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of sensitive data within its possession or control.

(ii) Although this section does not prescribe a specific number of policies and procedures a fiduciary must consider or adopt, the fiduciary must consider enough policies and procedures to show that he, she, or it genuinely is trying to protect the sensitive data in accordance with paragraph (a)(4).

(iii) The fiduciary must create and maintain the records described in paragraph (b)(3).

(2) **Necessary Policies and Procedures.** The policies and procedures described in subparagraph (b)(1)(i) must include:

(i) A plan for keeping all adopted policies and procedures (including the one described in this subparagraph) current;

(ii) A plan for vetting the data security practices of potential service providers; and

(iii) A plan for monitoring the data security practices of current service providers, including the frequency with which the fiduciary will monitor the service providers.

(3) **Recordkeeping.** The records described in paragraph (b)(2) must include:

(i) In the case of any considered policy or procedure, whether ultimately adopted or rejected, a detailed description of the process by which the decision to adopt or reject was made. This record must include, at a minimum:

(A) A description of any investigations into the costs and benefits of the considered policy or procedure;

(B) A description of any person involved in any way in the decision to accept or reject the considered policy or procedure (including persons whose involvement was limited to gathering or presenting information to the ultimate decisionmakers); and

(C) The time and money spent on considering the policy or procedure.

(ii) In the case of an adopted policy or procedure (including any amendments to or revocations of any existing policies or procedures):

(A) A brief description of the policy or procedure, both as proposed and as adopted;

(B) A detailed description of the reasons for accepting adoption of the final policy or procedure, including explanations of any changes to the policy or procedure from its originally proposed form; and

(C) A description of the plan for implementing the policy or procedure.

(iii) In the case of a rejected policy or procedure, a brief description of the considered policy or procedure and a detailed description of the reasons for rejecting its adoption.

(4) **Records Maintenance.**

(i) The fiduciary must keep the records required by paragraph (b)(2) for a period no shorter than five years.

(ii) In the case of any record relating to a currently adopted policy or procedure (including records of proposed amendments to or revocations of the policy or procedure), the fiduciary must keep the record for as long as the policy or procedure is in effect.

(c) **Duty with Respect to Selecting and Monitoring Service Providers.**

(1) **Requirements.**

(i) The fiduciary must not use any service provider unless it genuinely believes the service provider will adequately protect any sensitive data to which it has access. To accomplish this purpose, the fiduciary must comply with the vetting and monitoring requirements of subparagraphs (c)(1)(ii) and (c)(1)(iii).

(ii) Before hiring a potential service provider that will have any access to the sensitive data, the fiduciary must inquire into its data security practices, creating a record of the inquiry as described in paragraph (c)(2).

(iii) The fiduciary must regularly monitor the data security practices of any service providers that has access to any of the sensitive data. Whenever the fiduciary checks the data security practices of one of the plan's service providers, it must create a record of its observations as described in paragraph (c)(2).

(2) **Recordkeeping.** The records described in subparagraphs (c)(1)(ii) and (c)(1)(iii) must include:

(i) General information about the service provider, such as its name and contact information;

(ii) The names of any specific contacts for the service provider who provided the fiduciary with information about the service provider's data security practices;

(iii) A generalized description of the particular sensitive data the service provider needs to perform its duties and the reasons it needs the sensitive data;

(iv) Any information the fiduciary has learned about the service provider's data security practices, including the fiduciary's impressions of the service provider's data security practices;

(v) Copies of any documentation the fiduciary received from the service provider regarding the service provider's data security practices;

(vi) A brief description of the known data security practices of any of the service provider's competitors that the fiduciary has also contacted or examined;

(vii) A brief description of any factors other than data security that weigh for or against using the service provider; and

(viii) Any other information the fiduciary believes would be appropriate.

(3) **Records Maintenance.** The fiduciary must keep the records described in paragraph (c)(2) for a period no shorter than five years.

(d) **Combining Records.** If an employee benefit plan has more than one fiduciary, the fiduciaries of the plan may elect to keep a single set of records (as required by paragraphs (b)(2) and (c)(2) of this section) for the plan rather than keeping separate records as individual fiduciaries.

(e) **Burden of Proof.** The fiduciary shall bear the burden of proving he, she, or it complied with the requirements of this section.

(1) To meet his, her, or its burden under this subsection, the fiduciary must make two showings:

(i) The fiduciary complied with the objective, technical requirements of this section, such as its recordkeeping obligations; and

(ii) The fiduciary complied with the purpose of this section, as defined in paragraph (a)(4), by having the honest goal of protecting sensitive data through the development of tailored policies and procedures.

(2) The following factors, none of which is singularly determinative, shall help guide any inquiry under subparagraph (e)(1)(ii):

(i) The fiduciary's compliance with the objective, technical requirements of this section;

(ii) The amount and nature of sensitive data maintained by the employee benefit plan;

(iii) The employee benefit plan's needs with respect to its sensitive data;

(iv) The sophistication of the particular fiduciary;

(v) The resources available to the particular fiduciary; and

(vi) Any other evidence, considering the particular circumstances of each fiduciary, tending to show whether the fiduciary seriously considered its data security obligations under this section.

(f) **Definitions.** For purposes of this section, the following definitions apply:

(1) **Adopt.** The term "adopt" means to put a policy or procedure for protecting sensitive data into writing, implement it, and keep it current.

(2) **Consider.** The term "consider" means to examine a proposed policy or procedure and, after genuinely assessing its advantages and disadvantages, adopt or reject it.

(3) **Sensitive Data.** The phrase "sensitive data" means any information about the participants of an employee benefits plan. Examples include the participants' contact information, account information, medical information, or employment information.

(4) **Service Provider.** The phrase "service provider" means any entity or natural person that provides services of any kind to an employee benefit plan, except that it shall not include the employees or fiduciaries of the plan itself.