CHAPTER 6

Navigating the Cryptic Waters of Cybersecurity for Protecting Employee Benefit Plan Data and Adhering to Comprehensive Cybersecurity Policies and Procedures to Mitigate Risk

MICHELLE CAPEZZA*

Synopsis

---

* Michelle Capezza is Of Counsel with Mintz in the Employee Benefits & Executive Compensation practice. For more than 25 years, she has represented a range of clients in ERISA, employee benefits, and executive compensation matters including qualified retirement plans, ERISA fiduciary responsibilities, nonqualified deferred compensation arrangements, employee welfare benefit plans, equity/incentive programs, and benefits issues that arise in corporate transactions, across various industries. She also advises clients on the implications of increased automation and artificial intelligence in the workplace and the related employee benefits and compensation considerations for a changing workforce. For many years, Ms. Capezza has been recommended for her work in The Legal 500 United States, selected to the New York Metro Super Lawyers and Top Women Lists, and she has been ranked in Chambers USA 2022, 2023.

§ 6.01 INTRODUCTION

As of the end of the first quarter of 2023, almost $10 trillion in assets were held in U.S. employer-based defined contribution plans, with $6.9 trillion of that amount held in 401(k) plans.[1] Millions of Americans rely on these retirement programs for retirement security. Yet, for these retirement plans, as well as all types of employee benefit programs, plan participant data and accounts are at risk from data breach and/or theft. Plan sponsors and fiduciaries provide plan participant data to various service providers, and individual plan participants are often interacting online and with plan service provider representatives to manage their accounts. There are many access points for nefarious individuals to steal participant information and account assets.

In addition, the U.S. laws governing data privacy and security continue to evolve. While a uniform federal law may pass in the future, the current absence of a uniform federal law requires employers to navigate varying state and local, and even international, laws on data privacy and security compliance requirements, data breach notification procedures, and enforcement regimes with respect to the personal information and data of their employees and business customers. For example, the California Privacy Rights Act (CPRA) which became effective on Jan. 1, 2023 and amended the California Consumer Privacy Act (CCPA), provides robust rules concerning individual data rights modeled after the European Union's General Data Protection Regulation (GDPR), and more states are passing laws similar to the CPRA in the U.S.[2] These laws often include carve-outs for data that is protected under other laws such as protected health information collected by a covered entity (which includes a group health plan) or a business associate that may be protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and the applicable regulations. These types of carve-outs require further navigation of these laws and coordination for compliance. Thus, there is a tangled web of employer responsibilities with regard to the privacy and security of employee data in general that may be personally identifiable information or protected health information, which is further complicated in the context of employer-sponsored benefit plans where plan sponsors and fiduciaries have fiduciary

---

[1] See Investment Company Institute Quarterly Retirement Market Data report (June 14, 2023).

[2] Several new laws effective just in 2023 include The Colorado Privacy Act, The Connecticut Data Privacy Act, The Utah Consumer Privacy Act, The Virginia Consumer Data Privacy Act.

responsibilities to act prudently under the Employee Retirement Income Security Act of 1974, as amended ("ERISA"). ERISA is silent on the issue of cybersecurity and plan participant data, however, recent guidance at a minimum invokes fiduciary responsibility to mitigate benefit plan cybersecurity risks.

In the context of retirement plans, a best practices framework for cybersecurity was issued by the Employee Benefits Security Administration of the Department of Labor (DOL) on April 14, 2021 in three parts: (i) Tips for Hiring a Service Provider, (ii) Cybersecurity Program Best Practices, and (iii) Online Security Tips[3] (collectively, the "DOL Cybersecurity Best Practices"). This DOL Cybersecurity Best Practices guidance was issued almost ten years after the first ERISA Advisory Council report addressing privacy and security issues affecting employee benefit plans,[4] and states that ERISA plan fiduciaries have, at a minimum, a responsibility to mitigate cybersecurity risk.

Given that ERISA plan fiduciaries are held to high standards and must act in the best interest of the plan participants and beneficiaries, a failure to implement any cybersecurity measures to mitigate cybersecurity risk would not be prudent and would be negligent. The development of, and adherence to, cybersecurity best practices for plan governance should provide plan fiduciaries with a formidable defense against assertions of fiduciary breach and will serve as a layer of protection for the security of participants' and their beneficiaries' data and accounts. Yet, since the DOL Cyberse-

---

[3] On June 26, 2023, the Assistant Secretary at EBSA published "8 Tips for Protecting Your Retirement Savings Online" to reduce the risk of fraud or loss to retirement accounts as part of Internet Safety Awareness Month. These tips reiterate the need to register and monitor online accounts, use strong and unique account passwords, use multi-factor authentication, maintain updated contacted information, avoid use of public wi-fi to check accounts, be mindful of phishing scams, maintain updated antivirus software and apps, and know how to report identity theft and cybersecurity incidents. The tips also inform that plan fiduciaries have responsibility to take steps to protect the plan against cybersecurity risks including ensuring that recordkeepers and other service providers responsible for plan-related IT systems and data appropriately safeguard information. The tips also include the contact information for the benefits advisor at EBSA online at askebsa.dol.gov or by calling 1.866.444.3272.

[4] The Advisory Council on Employee Welfare and Pension Benefit Plans (ERISA Advisory Council) was established under Section 512 of ERISA to advise the Secretary of Labor. The 2011 ERISA Advisory Council Report on Privacy and Security Issues Affecting Employee Benefit Plans (November 2011) addressed privacy and security issues affecting employee benefit plans other than health care benefit plans. The ERISA Advisory Council focused on the privacy and security of benefit data and personal information in light of the dramatic changes in technology and its use in employee benefit plan management, and examined potential breaches of the technological systems used in the employee benefit industry, the misuse of benefit data and personal information, and the impact on plan sponsors, service providers and participants and beneficiaries. The Council recommended that the DOL (1) provide guidance on the obligation of plan fiduciaries to secure and keep private the personally identifiable information of participants and beneficiaries; (2) develop educational materials and outreach efforts for plan sponsors, participants, and beneficiaries to address these privacy and security issues; and (3) include in their outreach and educational materials information regarding elder abuse related to benefit plans.

0004 [ST: 6-1] [ED: 100000] [REL: 2023] **Composed:** Tue Sep 12 19:48:19 EDT 2023
XPP 9.6.2.0 SC_01125 llp 1646 [PW=486pt PD=648pt TW=384pt TD=528pt]
VER: [SC_01125-Master:04 Aug 23 02:10]**[MX-SECNDARY:** 12 Sep 23 12:15]**[TT-:** 29 Jul 21 00:02 loc=usa unit=ch0006v2023] **0**

curity Best Practices were issued, plan sponsors and fiduciaries have strived to understand the implications of the guidance on their fiduciary responsibilities, their application with respect to all of their employee benefit programs, and the ability of cyberinsurance and/or other contractual provisions to provide desired protections.

In the midst of navigating these considerations and attempting to prepare cybersecurity policies and procedures, additional complexities have emerged. Technology keeps advancing, creating increased layers of consideration and providing further avenues for loss of privacy and compromised security. Various applications (Apps) are utilized to collect, store and transmit personal financial or health data and aggregate information with employee benefit plans data and participant account information. The use of artificial intelligence (AI) tools in the workplace is increasing, including AI tools that can assist with personalized benefit selection to create a personalized benefits package based on predictions of future needs as a result of past behaviors or utilization. Chatbots can be deployed to answer benefit plan inquiries following collection of personalized information. In addition, the rise of digital assets such as cryptocurrencies as plan investments poses new challenges with respect to privacy and security of retirement accounts. Whereas a few years ago there may have been concern about protecting an employee's personally identifiable information such as name, address, birth date, and social security number data, this information is so widely available that it is not even the most valuable to cyber criminals. Even protected health information which is subject to HIPAA protocols seems not so private given the fact that the same medical information can be collected, stored, and transmitted with respect to benefits other than group health plan benefits, such as disability plans or leave programs which are not considered covered entities subject to the HIPAA requirements. Remote and hybrid work models also increase the risk of more data collection through technology and data exposure. Clearly, there are many angles from which data privacy and security can be breached, and, with AI being used in the workplace and benefit plan administration, where personal employee data can not only be collected, but also collated and analyzed to track and predict behaviors and related costs per individual, this leaves an even broader data footprint about plan participants. It is a new frontier of data privacy and security risk.

Plan sponsors and fiduciaries must be sensitive to all of the foregoing considerations and use them to inform their prudent decision making when it comes to the handling of their employee benefit plan participant and beneficiary data. This data must be secured, service providers and vendors must be vetted for their privacy and security controls and protocols, service agreements and contractual arrangements must address cybersecurity and scope of liability of the parties and indemnification rights, cyberinsurance should be obtained, and employees should be educated about protecting their own information and benefit accounts. Plan sponsors and fiduciaries should be familiar with the DOL Cybersecurity Best Practices, have already adopted and implemented

cybersecurity policies and procedures, and be in a position to continue to monitor that they are being followed and updated as appropriate. Plan sponsors and fiduciaries must also be able to demonstrate to government and plan auditors that cybersecurity controls are in place and followed, and some plan sponsors have already had to respond to DOL audits of their cybersecurity policies and procedures. Given the complexities and challenges involved, however, and the global pandemic, many have not yet adopted such protocols. The purpose of this article is to provide a framework for designing such cybersecurity policies and procedures as well as considerations for updating existing protocols.

§ 6.02 ESTABLISHING A FRAMEWORK FOR EMPLOYEE BENEFIT PLAN CYBERSECURITY POLICIES AND PROCEDURES

[1] Overview

As stated above, the DOL Cybersecurity Best Practices that were issued in 2021 addressed cybersecurity for ERISA governed retirement plans. This has left open the question about plan sponsor and fiduciary responsibilities with respect to other ERISA benefit plans, as well as plan sponsor responsibility for non-ERISA governed benefit programs. As raised in the 2011 ERISA Advisory Council Report, there are many ways that the requirements set forth in all applicable laws concerning privacy and security of employee data can apply in the context of managing data in employee benefits and related programs[5]. Complexities related to these laws can also arise in the context of plan distributions, especially in cases of identity theft, and when plan participant data can be transmitted in a myriad of ways, such as in connection with auto-portability programs which were codified in SECURE 2.0 Act,[6] and participant data and account information must be provided to the Retirement Lost and Found database under the SECURE 2.0 Act[7]. Plan participant data can also be transmitted to a service provider

---

[5] The 2011 ERISA Advisory Council Report acknowledged that ERISA does not directly address whether and how employee benefit plans should protect personally identifiable information, there has not been any jurisprudence concerning the potential of ERISA preemption of state laws and ERISA's preemption provision may not reach many of these state laws. Thus, the Council believes that as state laws are developed in the area of privacy of financial data and other personally identifiable information, including data breach notification laws, plan administrators will need to be mindful of these laws and adjust their administrative practices accordingly. Thereafter, the 2016 ERISA Advisory Council Report on Cybersecurity Considerations for Benefit Plans (November 2016) focused on information that would be useful to plan sponsors, fiduciaries and their service providers in evaluating and developing a cybersecurity program for their benefit plans.

[6] On December 29, 2022, the SECURE 2.0 Act passed as part of the Consolidated Appropriations Act, 2023 (SECURE 2.0 Act). Section 120 of the SECURE 2.0 Act codifies the permissibility of automatic portability transactions for certain retirement accounts.

[7] Section 303 of the SECURE 2.0 Act amends Part 5 of subtitle B of title I of ERISA to add a new Section 523 of ERISA providing for a Retirement Savings Lost and Found effective no later than December

for other benefits such as a disability plan or commuter benefit program, or employee data can be transmitted from employers to state auto-IRA programs. Thus, employee information and data must be secured under multi-layers of requirements arising from all different laws and best practices, and a violation of one of these layers or prongs, as applicable, as if navigating a massive flow chart of rules and regulations, can expose an employer, plan sponsor and/or fiduciary to different penalties and enforcement regimes depending on which arm of the flow chart one finds itself as a result of a cybersecurity breach incident.

More recently, the December 2022 ERISA Advisory Council Report on Cybersecurity Issues Affecting Health Benefit Plans[8] noted the confusion in the employee plan industry concerning whether the DOL Cybersecurity Best Practices apply to both retirement and health benefit plan sponsors and providers. The ERISA Advisory Council (the "Council") cited that the health care sector is one of the biggest targets for cyberattacks and that the HIPAA privacy and security rules have not kept up with the emerging cybersecurity threats, including ransomware[9]. Some Council members felt that given the similarities in the DOL's Cybersecurity Best Practices with HIPAA's security standard requirements, DOL should identify where the HIPAA requirements and the DOL guidance overlap before the DOL applies its DOL Cybersecurity Best Practices to health plans. In addition, the Council advised that since most of the security risks lies with third party administrators, insurers and other service providers, rigorous protocols should be in place for selection and monitoring of any service provider collecting, transmitting, handling or storing personally identifiable information or

---

29, 2024 (Retirement Savings Lost and Found). The goal of the Retirement Savings Lost and Found is to allow individuals to locate their ERISA-governed defined benefit or defined contribution retirement plan in order to make a claim for benefits owed to them under the plan.

[8] *See* The Advisory Council on Employee Welfare and Pension Benefit Plans Report to the Honorable Martin Walsh, United States Secretary of Labor on Cybersecurity Issues Affecting Health Benefit Plans (December 2022).

[9] The 2022 ERISA Advisory Council Report notes that in 2021, 349 data breaches affecting personal health information of 500 or more individuals and involving health care entities and their business associates covered by HIPAA were reported to the U.S. Department of Health and Human Services, more than three-fourths of those involved hacking/IT incidents, including 39 incidents directly involving health plans and affecting 4.7 million people. During the first ten months of 2022, there were 38 such incidents involving health plans affecting at least 1.9 million people. Retirement systems are also vulnerable. In early June 2023, the staff at the California State Teachers Retirement System (CSTRS) and the California Public Employees Retirement System (CALPERS) received notification from a vendor, PBI Research Services, that a hacker had punched through a weakness in the software code of a data transfer platform it used to securely share information and the unauthorized actor accessed files contained in its MoveIt appliance in May 2023. The ransomware group Clop, or C10p, claimed to have infiltrated the MoveIt secure file transfer, a product of Progress Software, and stole information from hundreds of government agencies, universities, businesses and other entities around the world. The vendor, PBI, had been engaged to assist with identifying members who had died to prevent overpayments and other errors.

protected health information, and DOL guidance addressing health plan fiduciaries' duty to act prudently should include a duty to ascertain that their health plan service providers have prudent cybersecurity procedures and that service agreements adequately address this issue. The Council made several recommendations in its 2022 Report including that the DOL (i) explicitly specify that plan fiduciaries must act prudently with regard to cybersecurity risks of all employee benefit plans (not just pension plans), (ii) clarify that health plan fiduciaries must ascertain that their health plan service providers have cybersecurity procedures to protect against risks, (iii) explain how compliance with HIPAA privacy and security requirements overlaps with the DOL Cybersecurity Best Practices, (iv) regularly review and update its DOL Cybersecurity Best Practices guidance to ensure it keeps up with the evolving cybersecurity and technological changes, and (v) provide educational materials to health plan sponsors and fiduciaries regarding cybersecurity, especially for small and medium-sized plan sponsors that lack cybersecurity advisors.

In light of the foregoing, it is essential for plan sponsors and fiduciaries to ensure that they have adopted an approach for addressing cybersecurity for employee benefit plan data that is being followed and updated as appropriate.

[2] Adopt and Follow Policies Modeled after the DOL Cybersecurity Best Practices

[a] Develop a Prudent Process for Selecting and Monitoring Service Providers

A starting point for plan sponsors and fiduciaries is to adopt cybersecurity policies and procedures for their employee benefit plans that, at a minimum, take into account the considerations set forth in the DOL Cybersecurity Best Practices wherein the DOL stated that responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks. Although cybersecurity was not contemplated when ERISA was passed into law, this duty to mitigate cybersecurity risks appears to fit squarely within the general fiduciary duty of prudence. Based on this guidance, plan sponsors and fiduciaries should address the following considerations in their cybersecurity policies and procedures as a baseline that can be expanded and updated as cybersecurity issues and the legal landscape evolves.

The DOL Cybersecurity Best Practices recognize that plan sponsors of retirement plans rely on service providers to confidentially maintain plan records and participant data, and to ensure that plan accounts are secure. Therefore, plan sponsors and fiduciaries must select service providers that follow strong cybersecurity practices and continually monitor that they adhere to these practices. The DOL Cybersecurity Best Practices offer tips to assist plan sponsors and fiduciaries meet their fiduciary responsibilities in selecting and monitoring service providers. Regardless of whether the DOL clarifies that it meant for these tips to apply solely to retirement plans or not,

it would be prudent to implement these tips with respect to all employee benefit plan management. These tips include the following due diligence points for plan sponsors and fiduciaries:

(a) Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions,

(b) Seek service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity,

(c) Ask the service provider how it validates its practices, what levels of security standards it has met and implemented, and ensure contract provisions provide a right to review audit results demonstrating compliance with the standard,

(d) Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services,

(e) Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded,

(f) Determine if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account),

(g) Negotiate service agreements that (a) require ongoing compliance with cybersecurity and information security standards, (b) address the service provider's responsibility for information technology ("IT") security breaches, (c) require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures, (d) clearly address the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse, (e) address data breach procedures including how quickly the service provider would provide notification of any cyber incident or data breach, and its cooperation to investigate and reasonably address the cause of the breach, (f) address the service provider's obligations to

> meet all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information, and (g) address insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage.

The second part of the DOL Cybersecurity Best Practices, which is addressed below, provides further detail on what plan sponsors and fiduciaries should evaluate related to a service provider's cybersecurity program. Again, although these tips were geared toward selection and monitoring of retirement plan service providers, it would be prudent to apply a similarly high level of due diligence on all employee benefit plan service providers that are collecting, handling, transmitting and/or storing participant data. Oftentimes, plan sponsors have IT, data privacy, vendor procurement and risk management specialists that are well-suited to review an employee benefit plan service provider's audit reports (such as SOC 1, SOC 2 and SOC 3 reports)[10] as well as service contract terms and insurance coverages. These professionals often have developed specific data privacy addendums that should be added to all vendor contracts or need to be negotiated with service providers. Plan fiduciaries should engage with these teams of professionals when a service provider is being reviewed in an RFP process, and as part of ongoing monitoring protocols. If an organization does not have this expertise in-house, it would be prudent to ensure that professionals with this expertise are engaged to assist.

Another challenge with vetting service providers concerns the additional third parties that a particular service provider may utilize when providing services to a benefit plan. All service agreements should seek indemnification for the negligence or gross misconduct of any subcontractor or agent of the service provider and an assurance that the service provider will hold its subcontractors or agents to the same privacy and security standards it upholds. It is not always clear, however, where participant data and account information is located at a point in time or where there is a cybersecurity vulnerability. Often data is uploaded to the cloud and there may be third parties managing those systems. Consider another example concerning the phishing incident that occurred in March 2023 related to the employee email account of a well-known auto-portability provider that assists with the portability of small balance cash-outs

---

[10] Systems and Organization Controls (SOC) 1 reports on the controls of a service organization that are relevant to the user organization's internal controls over financial reporting. SOC 2 and SOC 3 reports are used to meet vendor risk management requirements that customers may request surrounding security. The SOC 2 report is more robust than the SOC 3 report, and reports on the effectiveness of the controls of the service organization related to operations, based on the selected trust services criteria of security, confidentiality, availability, processing integrity and privacy and can also include other suitable criteria, such as HITRUST, the HIPAA Security Rule and others.

from terminated plan accounts and defaulted individual retirement accounts[11]. This incident required the provider to alert more than 10,500 individuals on May 12, 2023 that their personal data (including their names, Social Security numbers and individual retirement account (IRA) numbers) may have been breached. The auto-portability provision in the SECURE 2.0 Act have now codified the use of these negative consent auto-portability transactions, which will increase their use. While the auto-portability provider reported that this data breach incident did not affect the network that it is establishing with large retirement recordkeepers to facilitate these auto-portability transactions, and assured that it is evaluating additional safeguards to mitigate recurrence of this type of event, this incident is another example of the potential cybersecurity vulnerabilities lurking in the retirement plan distribution process.

Given the SECURE 2.0 Act's provisions for auto-portability transactions, as well as its provisions for an upcoming Retirement Savings Lost and Found database which will require plan sponsors to remit various types of information to this database[12], including information related to small balance cash-outs, plan sponsors and fiduciaries should also consider how their cybersecurity policies and procedures address the plan distribution process, any service providers involved in that process, and make desired updates. With respect to general plan distributions, procedures may require updates around (a) the verification and authentication process of participant identity in connection with distribution requests, (b) waiting periods before distributing account assets, (c) monitoring related service provider protocols and security measures concerning plan distributions, breach and response procedures, and (d) updating service agreements for indemnification, limitations of liability, insurance for cybersecurity issues, and any loss guarantees provided by the service provider. Security measures

---

[11] See, Capezza, "Another Vulnerability for Cybersecurity of Retirement Plan Data: Auto-Portability", The National Law Review, May 26, 2023).

[12] The DOL information security program also needs improvement. See FY 2021 FISMA DOL INFORMATION SECURITY REPORT: INFORMATION SECURITY CONTINUOUS MONITORING CONTROLS REMAIN DEFICIENT (January 28, 2022). Under the Federal Information Security Modernization Act of 2014 (FISMA), the U.S. Department of Labor (DOL) Office of Inspector General (OIG) is required to perform annual independent evaluations of the Department's information security program and practices. This effort assesses the effectiveness of information security controls over information resources that support federal operations and assets, and it also provides a mechanism for improved oversight of information security programs. This includes assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems. OIG contracted with KPMG LLP (KPMG) to conduct an independent audit on DOL's fiscal year (FY) 2021 information security program for the period October 1, 2020, through September 30, 2021 and evaluated security controls in accordance with applicable legislation, guidelines, directives, and other documentation. Findings were also based on testing the security controls and targeted vulnerability assessments. KMPG found weakness that demonstrated that the information security program had not achieved a Managed and Measurable (Level 4) in three of the five Cybersecurity Functions: Identify, Detect, and Recover.

around plan distribution processes should be discussed when selecting service providers and those procedures should be monitored. In connection with auto-portability procedures, more diligence may be needed on the parties involved in these transactions. Moreover, as more guidance is issued regarding implementation of the SECURE 2.0 Act provisions, including the auto-portability provisions and the Retirement Savings Lost and Found database, cybersecurity policies and procedures will likely need to be amended to address these processes.

Employee benefit plan cybersecurity policies and procedures should also address and be updated for cybersecurity issues related to any applicable investment options such as digital assets or services that introduce new technologies through a benefit program. For example, in Compliance Assistance Release No. 2022-01, the DOL cautioned against offering 401k plan participants access to digital asset investments such as cryptocurrencies due to their volatile nature and the significant risks they pose with respect to fraud, theft and loss, including special vulnerabilities to hackers. In addition to assessing the prudence of offering access to such investments, plan sponsors and fiduciaries must carefully review service provider agreements for disclaimers related to the service provider's liability associated with a cyber incident involving digital assets. These types of risk shifting provisions may serve as sufficient reason to not permit access to such investments[13]. However, given the evolving legal landscape for digital assets, it is more likely that they will need to be evaluated as plan investment options in the future and accounted for in plan cybersecurity policies and procedures.

There are also various technologies and services to consider with respect to benefit programs. There is a myriad of financial and health oriented Apps that can be offered to plan participants that collect participant data and may aggregate such information with data in various plan accounts or facilitate unauthorized disclosures.[14] Any Apps services should be reviewed and evaluated by the plan sponsor's IT and security advisors and usage of such Apps factored into the prudent selection process and cybersecurity protocols. Moreover, as AI-tools, chatbots and robots continue to evolve, they too will used in the workplace with increasing regularity on a large scale, interacting with employees and collecting, handling, storing and transmitting large amounts of data. The ability of AI-tools and bots to assist employees in answering their

---

[13] For further discussion regarding plan investments and cybercrime, see Heidi J. Schmid, Protecting Plan Assets from Cybersecurity Risk—the Evolving Challenge, Vol. 36, No. 1 Benefits Law Journal, Spring 2023.

[14] See also the Federal Trade Commission Notice of Proposed Rulemaking and Request for Public Comments (May 18, 2023) seeking to amend the Health Breach Notification Rule to include unauthorized disclosure in the definition of breach of security which would address unauthorized sharing of consumer health data through Apps to advertising technology solution providers.

questions and providing personalized benefits selection indicates that the data accumulated by these tools is highly sensitive and related data security measures must be addressed.

[b] Ensure that Service Providers Maintain and Follow Prudent Cybersecurity Programs

The DOL Cybersecurity Best Practices include guidance for use by recordkeepers[15] and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. This second part of the guidance provides further detail on what plan sponsors and fiduciaries should evaluate related to a service provider's cybersecurity program. For example, plan sponsors and fiduciaries should determine that the service provider:

(a) Has a formal, well documented cybersecurity program that is reviewed at least annually to identify and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information and protects the security of the IT infrastructure and data stored on the system from unauthorized access, use, or other malicious acts.

(b) Conducts prudent annual risk assessments.

(c) Has a reliable annual third party audit of security controls by an independent auditor that can assess an organization's security controls and provide a clear, unbiased report of existing risks, vulnerabilities,

---

[15] In October 2022, the SPARK Institute also published its Plan Sponsor and Advisor Guide to Cybersecurity, SPARK Data Security Best Practices: Seventeen Control Objectives. Recognizing the rising threat of retirement account take-overs and fraud, the SPARK Institute established Seventeen Control Objectives to set a base of communication between recordkeepers and the public through third party audits of cybersecurity control objectives. SPARK Institute recommends that when plan sponsors and fiduciaries review or select a recordkeeper, that they first request a copy of their SPARK cybersecurity reports for each of the Seventeen Control Objectives which can assist in serving as a basis for evaluation of the service provider's cybersecurity capabilities. The Seventeen Control Objectives include (1) completed risk assessments, (2) implemented information security policies, (3) demonstrated leadership for organizational security, (4) maintained asset management in a formal system, (5) security of personnel/background checks, (6) protected physical access to assets, (7) protected networks and systems, (8) access controls, (9) conduct penetration tests, (10) documented/routinely tests cyber incident procedures, (11) business continuity and business resiliency plans, (12) compliance with applicable privacy obligations, (13) mobile policies, (14) encryption for data at rest and in transit, (15) addressed security of suppliers, (16) ensure cloud security, and (17) procedure to detect, prevent and respond to ransomware events. An independent third party auditor of the service providers can report on these objectives in a SOC 2 report, HiTrust Certification, ISO Certification or Agreed-Upon-Procedures (following the Association of International Certified Professional Accountants guidance). The audit report must identity the primary applications and processing systems that support the services offered and what systems are within the scope of the audit and which systems are not.

and weaknesses.

(d) Clearly defines and assigns information security roles and responsibilities managed at the senior executive level and executed by qualified personnel such as a Chief Information Security Officer.

(e) Has strong access control procedures to guarantee that users are properly authenticated and authorized to have access to IT systems and data.

(f) Ensures that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments and provide contractual protections.[16]

(g) Conducts periodic cybersecurity awareness training at least annually for all personnel and educate everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat[17].

(h) Implements and manages a secure system development life cycle (SDLC) program that ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort.

(i) Has an effective business resiliency program addressing business continuity, disaster recovery, and incident response to recover from disruptions and security incidents.

(j) Encrypts sensitive data, stored and in transit.

(k) Implements strong technical controls in accordance with best security practices including updated hardware, software, firmware, firewalls, intrusion detection and prevention tools, antivirus software, and patch management.

(l) Appropriately responds to any past cybersecurity incidents including informing law enforcement, notifying the appropriate insurer, investigating the incident, giving affected plans and participants the information necessary to prevent/reduce injury, honoring any contractual or legal obligations with respect to the breach, including

---

[16] Problematically, it is difficult for the plan sponsor and fiduciaries to know who their directly contracted service provider is utilizing as a third-party cloud provider. Diligence is necessary to ascertain these relationships, review applicable protocols of all service providers, and negotiate for service agreement protections.

[17] It is important to note that the employees of the service providers must also undergo the requisite training and diligence inquiries on this aspect of the service provider's controls are necessary.

complying with agreed upon notification requirements, and fixing the problems that caused the breach to prevent its recurrence.

As noted in the 2022 ERISA Advisory Council Report, health plan fiduciaries should also ascertain that their health plan service providers have cybersecurity procedures to protect against risks. Further, it is imperative to drill into the additional layers of third-parties, agents and subcontractors, and even Apps and other tools with access to this data and the protocols deployed by these entities. Any RFPs to change service providers must address cybersecurity, document the diligence efforts, address data retention and storage following termination of services, and negotiate applicable service agreement provisions. Moreover, there should be a protocol in place to coordinate between these service providers and the plan sponsor in the event of a cybersecurity incident. There must be robust procedures on all sides that are monitored and updated to address privacy and security and to seal any gaps.

[3] Educate and Train Employees and Plan Participants

Educating employees and plan participants in cybersecurity matters that are related to their information and data is also critical. The DOL Cybersecurity Best Practices include online security tips for individuals to follow in order to reduce the risk of fraud and loss to retirement accounts. These tips could also be provided to employees and all employee benefit plan participants as part of a larger educational program. These tips include:

(a) Registering for and regularly monitoring online accounts;

(b) Use of strong and unique passwords;

(c) Use of multi-factor authentication;

(d) Closure or deletion of unused accounts;

(e) Being wary of free wi-fi;

(f) Beware of phishing attacks;

(g) Using antivirus software and keep Apps and software current; and

(h) Knowing how to report identity theft and cybersecurity incidents.[18]

Recordkeepers often have educational resources that can be offered to plan participants. Employers can also provide organization-wide webinars or cybersecurity preparedness courses to test employee knowledge and to facilitate test drills, including mock phishing exercises and other tests to help identify cyber risks. The 2022 ERISA Advisory Council Report also recommended that the DOL provide educational

[18] The FBI and the Department of Homeland Security have set up sites for reporting cybersecurity incidents: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view; https://www.cisa.gov/reporting-cyber-incidents.

materials to health plan sponsors and fiduciaries, including through updates to its *Understanding Your Fiduciary Responsibilities under a Group Health Plan* publication regarding cybersecurity. Plan service providers should also be expected to train their employees on these matters and have appropriate controls in place as noted above.

In addition to the required plan disclosures that must be provided to plan participants as prescribed under ERISA and the Code, plan sponsors and fiduciaries should consider developing plan communications that will enable eligible employees and plan participants to more fully understand how they can protect their information and benefit plan accounts from cybersecurity risks. Education concerning associated risks of utilizing Apps that collect data and interact with other plan accounts to aggregate data should also be considered. Even finding small ways to provide eligible employees and participants with quick and digestible educational tips in an ongoing manner will have a positive impact. A larger goal should be to provide more robust educational campaigns on cybersecurity.

§ 6.03 COORDINATE EMPLOYEE BENEFIT PLAN CYBERSECURITY POLICIES WITH ORGANIZATIONAL PROTOCOLS

Once the plan sponsor and fiduciaries have established a baseline approach to their cybersecurity policies and procedures for employee benefit plans, it is important for plan sponsors and fiduciaries to coordinate their efforts with the employer organization's data privacy and security professionals. Organizations, as employers, are subject to a myriad of state, local and other laws governing employee data privacy and security, and breach notification procedures. To the extent not already done so, the employer's compliance protocols that are in place should be leveraged and integrated into the employee benefit plan data management procedures. The employer's team of professionals, which may include members of IT (and designated cybersecurity leaders), legal, risk management, compliance, human resources, and vendor procurement, should review these Employee Benefit Plan Cybersecurity Policies and Procedures and ensure that overall organizational data privacy and security policies that have been adopted for compliance with all applicable data privacy and security laws are reflected and integrated into such policies.

To comply with applicable laws as an organization, the team would have identified all employee data that is collected, transmitted, processed, stored, and the encryption and data retention protocols in place for same. It will be difficult to assert that ERISA preemption applies to these applicable state data privacy and security and other laws with respect to employee data handled for employee benefit plan administration. Even if an ERISA preemption argument could be made, not all programs are ERISA-governed plans and, more likely than not, state and other laws governing data privacy and security are not directed at employee benefit plans. It will be difficult for an

employer to argue that it was not required to comply with such laws with regard to employee benefit plan data when the employer was otherwise required to protect employee data.

The Employer's governing body should also be apprised of the plan fiduciaries' actions with respect to ensuring cybersecurity of employee benefit plan data. If an employer's Board of Directors ("Board"), for example, took action to delegate plan sponsor fiduciary responsibilities to specific individuals or to a benefits committee, the Board has an ongoing duty to monitor and ensure that those individuals are prudently carrying out their fiduciary responsibilities. The Board should ensure that resolutions have been adopted to properly reflect that delegations of fiduciary responsibility are in place and that those delegees periodically report to the Board regarding their plan management activities. In the event of a cybersecurity breach involving employee benefit plan data, the reporting and handling of such an incident should also be coordinated with the organization's data breach incident response protocols and the plan's policies should reflect alignment with organizational policies including Board or governing body notifications of a cyber incident.

In this evolving cybersecurity legal landscape, it would not be prudent for plan sponsors and fiduciaries to operate in a silo disjointed from the rest of the employer organization. The cybersecurity policies and procedures require multi-disciplinary expertise, and must address multi-jurisdictional concerns. Organizations must coordinate their efforts among relevant stakeholders, conduct periodic risk assessments, and self-audits, maintain updated systems, policies and procedures, and train employees to identify cybersecurity risks before they become data breach incidents. As previously stated, the current guidance indicates that ERISA plan fiduciaries have, at a minimum, a responsibility to mitigate cybersecurity risk. Given that ERISA plan fiduciaries are held to high standards and must act in the best interest of the plan participants and beneficiaries, development of, and adherence to, cybersecurity best practices for plan governance will serve to protect the plan fiduciaries from assertions of fiduciary breach and will serve to protect the data and accounts of participants and their beneficiaries.

§ 6.04 CYBERSECURITY INSURANCE CONSIDERATIONS

There are several ways in which plan sponsors and fiduciaries currently protect against losses with respect to employee benefit plans. Section 412 of ERISA requires that every fiduciary of a funded employee benefit plan that is subject to Title I of ERISA, and every person who handles funds or other property of such a plan, is bonded, unless covered by an applicable exemption. The bond requirement is intended to protect employee benefit plans from risk of loss due to fraud or dishonesty on the part of those persons (i.e., plan officials) who handle plan funds or other property,[19]

[19] A plan official must be bonded for at least 10% of the amount of funds he or she handles, subject

including for acts of larceny, theft or embezzlement. An employee benefit plan might also be a named insured to a company's crime bond but an ERISA rider would likely be needed to ensure that it provides the requisite coverage for those who handle plan funds.[20] Fiduciary liability insurance, on the other hand, generally insures the plan against losses caused by breaches of fiduciary responsibilities, and it is not required nor subject to Section 412 of ERISA.[21] A plan sponsor may also be able to indemnify the plan fiduciaries for asserted claims and costs so long as the fiduciary did not act with gross negligence or willful misconduct. Other types of insurance such as an errors and omissions policy will not necessarily provide coverage for ERISA breaches of fiduciary responsibility absent a specific rider for such claims. With advances in technology and the increase in cybercrimes, the coverage approaches related to cybersecurity insurance are of concern and being evaluated with more regularity.

The Council examined the issue of cybersecurity insurance in its December 2022 Report to the DOL on Cybersecurity Insurance and Employee Benefit Plans[22] and recommended that the DOL further review this topic due to its nuances and complexities as it relates to employee benefit plans. The Council made two specific recommendations in this Report. First, it recommended that the DOL should holistically study the various forms of loss risk-mitigation strategies before any guidance is issued, including cybersecurity insurance, fidelity/crime coverage, fiduciary liability coverage and third-party service provider contractual obligations (including indemnification and insurance). Further, the Council advised that the review should examine the evolving landscape of insurance coverage available, consider the various types of employee benefit plans, the probability of a cybersecurity incident based on the size of the organization or plan, the types of claims filed in connection with the cybersecurity incident and whether the plan or some other party would be responsible for financial

---

to a minimum bond amount of $1,000 per plan with respect to which the plan official has handling functions. The maximum bond amount that is required under ERISA with respect to any one plan official is $500,000 per plan (or $1,000,000 for plan officials of plans that hold employer securities). Importantly, the bond must be placed with a surety or reinsurer that is named on the Department of Treasury's Listing of Approved Sureties, Department Circular 570, or in certain cases, the bond may be placed with the underwriters at Lloyds of London. *See also* DOL Field Assistance Bulletin No. 2008-04 (November 25, 2008).

[20] See Q&A 29 of FAB 2008-04.

[21] Section 410 of ERISA permits a plan to purchase insurance for its fiduciaries or for itself covering losses occurring from acts or omissions of a fiduciary. Any such policy paid for by the plan must permit recourse by the insurer against the fiduciary in the case of a fiduciary breach. The fiduciary may be able to purchase at his or her own expense protection against the insurer's recourse rights. *See* DOL FAB 2008-04.

[22] *See* the Advisory Council on Employee Welfare and Pension Benefit Plans Report to the Honorable Martin Walsh, United States Secretary of Labor on Cybersecurity Insurance and Employee Benefit Plans (December 2022).

harm. Secondly, the Council recommended that the DOL should develop education for employee benefit plan fiduciaries concerning the various types of insurance coverage that is available to protect against losses resulting from cyber incidents due to the complexities of the insurance issues that are not well understood by plan fiduciaries. Given that this is an evolving area, this information needs to be shared on a wide-scale so that plan sponsors and fiduciaries understand the types of cyber threats, the types of losses covered by cyber-insurance versus other types of policies, the carve-outs, exclusions, deductibles and coverage limits for the named insured in these policies, and the role that the plan's own cybersecurity policies and procedures play in the application, underwriting, and/or renewal process for cyber-related insurance coverage.

In light of the foregoing, plan sponsors and fiduciaries should prioritize a review of their current ERISA bond, fiduciary liability and other insurance coverages, and contractual indemnification and limitation of liability provisions with respect to their employee benefit plans and third-party service provider relationships. The issue of cybersecurity insurance adds a new layer of complexity to an already existing area where there are knowledge and oversight gaps. Many organizations still confuse the fidelity bond with fiduciary liability insurance. Others may believe that they have coverage for ERISA breaches of fiduciary responsibility but they do not have a specific fiduciary liability policy, nor do they have an ERISA rider to other policies that might be able to cover such claims. The addition of cybersecurity insurance to the plan sponsor's array of insurance will need to be properly evaluated so that the stacked layers of protection are coordinated and the scope of coverage, carve-outs, and exclusions are understood by the necessary parties.

As noted by the Council, the plan sponsors and fiduciaries, as well as the third-party service providers, need to have strong cybersecurity controls, policies and procedures to protect against cyber incidents and to mitigate risks. It will be necessary to demonstrate that these protections are in place not only to parties such as the DOL, auditors and potential litigants, but also to insurance underwriters and claims reviewers. Adoption of cybersecurity policies and procedures that comport to the DOL Cybersecurity Best Practice guidance and an organization's overall data privacy and security procedures for employee data is critical. These policies and procedures must be consistently followed and updated for changes in the cybersecurity landscape and applicable law.

§ 6.05 POTENTIAL CLAIMS AND LITIGATION

A cybersecurity breach of plan participant data or retirement account assets, for example, can expose plan sponsors and fiduciaries to potential breach of fiduciary duty litigation risk as well as other potential liabilities. Litigation is this area is evolving and, to date, there is not a case that has opined that data is a plan asset to which a fiduciary duty to protect plan assets applies or whereby misuse or self-dealing regarding such

data could give rise to a prohibited transaction.[23] Yet, potential claims could run the gamut, including under Section 502(a)(2) of ERISA which provides a cause of action for breach of fiduciary duty for "appropriate relief"[24] under Section 409 of ERISA,[25]

---

[23] See e.g., Divane v. Northwestern University, No. 16 C 8157, 2018 WL 2388118 (N.D. Ill, May 25, 2018), aff'd No. 18-2569, 2020 WL 1444966 (7th Cir. March 25, 2020) (finding that participant data including contact information, age, and account asset size was not a plan asset because it was not property the plan could sell or lease to fund retirement benefits. See also, Harmon v. Shell Oil Company, 2021 WL 1232694 (S.D. Tex. Mar. 30, 2021) (where the Southern District of Texas was unable to conclude that participant data is a plan asset under ERISA). In Cassell v. Vanderbilt University, the plaintiffs brought both breach of fiduciary duty claims and claims for violations of prohibited transaction rules, alleging that the plan allowed service providers to use their positions as recordkeepers to obtain access to participants, learning their ages, length of employment, contact information, account sizes, and investment choices, and used that information in marketing lucrative investment products and wealth management services to participants as they neared retirement. The case settled but the settlement contained a provision requiring the plan's recordkeeper to refrain from using information about plan participants acquired in the court of providing recordkeeping services to the plan to market or sell products or services unrelated to the plan unless a request for these products or services I initiated by a plan participant (285 F. Supp. 3d 1056(M.D> Tenn. 2018)).

[24] ERISA Section 502(a)(2) claims have been brought in the context of fraudulent plan account distributions. For example, in Leventhal v. MandMarblestone Group, LLC, the plaintiff brought a claim against the defendant after the plaintiff's 401(k) account was fraudulently reduced from almost $400,000 to $0 (2019 WL 1953247 (E.D. Pa. May 2, 2019)). The plaintiff alleged that the defendant improperly distributed the funds to a bank account that was never authorized by the plaintiff and that the withdrawal of this substantial amount of money was never authenticated with forms or a signature from the plaintiff, and that the defendant did not implement its procedures in notifying the plaintiff of these strange requests or to verify the authenticity of these requests. Addressing the defendant's motion to dismiss for failure to state a claim, the court found that the plaintiffs sufficiently pleaded a breach of duty by alleging that the defendant failed to act with the requisite prudence and diligence where the defendants saw the peculiar nature and high frequency of the withdrawal requests that were to be distributed to a new bank account but failed to alert the plaintiffs or verify the requests. The court also relied on the fact that the defendant failed to implement the typical procedures and safeguards used to notify the plaintiffs of the strange requests and to verify the requests. The court also permitted the plan administrator to assert counterclaims against co-fiduciaries for contribution and indemnification, alleging their own carelessness See Leventhal, 2020 WL 2745740 (E.D. Pa. May 27, 2020). Similarly, the plaintiff in Berman v. Estee Lauder, No. 3:19-CV-06489 (N.D. Cal. Oct. 9, 2019) brought claims against the defendants alleging that the plan had allowed the plaintiff's $99,000 401(k) account to be fraudulently distributed to various bank accounts without the plaintiff's authorization. The plaintiff alleged that the defendants breached their fiduciary duty of loyalty and prudence by allowing the plan to make unauthorized distributions of plan assets, failing to confirm authorization for distributions with the plan participant before making distributions, failing to provide timely notice of distributions to the plan participant by telephone or email, failing to establish distribution processes to safeguard plan assets against unauthorized withdrawals, and failing to monitor other fiduciaries' distributions processes. This case settled in March 2020.

In Bartnett v. Abbott Laboratories, the plaintiffs' complaint asserted breach of fiduciary duty claims against the plan sponsor, other plan administrators, and recordkeepers seeking to recover $245,000 that was depleted from the plaintiff's retirement account in alleged unauthorized distributions by an impersonator

or Section 502(a)(3) of ERISA for "equitable relief,"[26] to denial of benefits claims under Section 502(a)(1)(B) of ERISA,[27] to state law claims for breach of state privacy

---

fraudulently accessing the plaintiff's online account. The court granted in part and denied in part the defendants' motions to dismiss the complaint (492 F.Supp. 3d 787, 802 (N.D. Ill. 2020), and the court later granted the defendants' motion to dismiss the amended complaint (2021 WL 428820 (N.D. Ill. Feb. 8, 2021).

See also, Disberry v. Employee Relations Comm. of the Colgate-Palmolive Co., Alight Solutions LLC and Bank of NY Mellon Corporation, 22 Civ. 5778 (CM) (S.D.N.Y. Dec. 19, 2022). In Disberry, a fraudster updated the plaintiff's contact information with the 401k plan recordkeeper, accessed the participant's online retirement account to request a full distribution to be made via direct deposit to a new bank account, and then contacted the representative to request a check distribution when the online transaction was not processed. In July 2022, plaintiff filed a Complaint in this action alleging one count against all defendants for breach of fiduciary duties of loyalty and prudence under Sections 409 and 502(a)(2) of ERISA in relation to (1) causing the plan to make unauthorized distributions, (2) failing to identify and investigate suspicious activities, (3) failing to halt suspicious distribution requests, (4) failing to confirm authorization for distributions, (5) failing to provide timely notice of a request for distributions to plaintiff, (6) failing to establish distribution processes to safeguard plan assets against unauthorized withdrawals, and (7) failing to monitor other fiduciaries' distribution processes and protocols. The court would not dismiss a motion asserting that the recordkeeper was not a fiduciary because it may have been a functional fiduciary directing the directed trustee to make the distribution, but this would still need to be decided. The court also noted that plaintiff might have considered an alternative claim against the recordkeeper for negligence as state law claims against non-fiduciaries are not preempted by ERISA.

[25] Section 409 of ERISA permits a plan to recover any losses resulting from a breach of fiduciary duty. It provides that a fiduciary is personally liable for losses caused to the plan, restoration to the plan of any profits that the fiduciary made by using plan assets, and other equitable or remedial relief as a court may deem appropriate, including removal of the fiduciary.

[26] ERISA Section 502(a)(3) is a catchall provision that can provide relief for injuries not adequately remedied elsewhere under ERISA Section 502. See Varity Corp. v. Howe, 516 U.S. 489, 515 (1996). Potential relief for cybersecurity breach claims could arise under "surcharge" theories where there is a breach of trust, and actual harm suffered caused by the breach. Suit might also be brought by a plan fiduciary against a service provider to enjoin a certain practice, such as sending data to a third party cloud provider. It remains to be seen if equitable relief can be invoked where damages are not so concrete, as is the case with identity theft.

[27] When an individual wants what was supposed to have been distributed under a plan, the appropriate remedy is under Section 502(a)(1)(B) of ERISA. See Hager v. DBG Partners, Inc., 903 F.3d 460, 469 (5th Cir. 2018). In *Foster v. PPB Industries Inc.*, (693 F.3d 1226) (10th Cir. 2012), the Tenth Circuit upheld a decision in which the plan administrator denied the plaintiff's request for additional benefits on the grounds that: plan had in place all the necessary and proper security measures, the benefits were paid under all plan terms and requirements, and the plaintiff's loss of benefits was due to the plaintiff's own failure to comply with the plan's address change requirements as well as the fraudulent conduct of the plaintiff's ex-spouse. The plaintiff challenged this determination in the district court, saying the money had been forfeited in violation of ERISA, and demanded from the defendant a distribution of the plaintiff's share of the plan, but the defendants denied this request. The Tenth Circuit relied on the fact that the plan administrator notified the plaintiff and other participants through the SPD of their ability to access their account information electronically and to keep their address information current, as all Plan correspon-

laws, breach of contract and negligence, as well other applicable laws.[28] Even if a lawsuit is unsuccessful for a plaintiff, plan sponsors and fiduciaries will spend an inordinate amount of time and incur substantial costs defending such suits, especially if they cannot clearly demonstrate that the appropriate cybersecurity policies and procedures were established, consistently followed and monitored. When plan sponsors and fiduciaries establish procedures to safeguard participants' data and mitigate risks, and abide by those procedures, they can assist in preventing cybersecurity breach and provide a better safeguard against liability for these claims.

Given this is an evolving area of litigation, which could develop into the proliferation of cases as seen in the area of 401(k) fee litigations, the question often arises as to whether plan documents, such as 401(k) plans, could specifically provide for arbitration of ERISA fiduciary breach claims related to cybersecurity breaches. Following the U.S. Supreme Court's decision in *LaRue v. DeWolff, Boberg & Associates, Inc.*[29] which allowed for individual relief for a fiduciary breach causing losses in an individual account under Section 502(a)(2) of ERISA rather than requiring availability of only plan-wide relief for such claims, and also an unpublished decision in the Ninth Circuit compelling individual arbitration of the plaintiff's ERISA Section 502(a)(2) claims for individual account losses,[30] it seemed that it may be possible to hard wire into a plan document the arbitration of participant claims related to cyber incidents. This case law, however, is also evolving with more recent cases invalidating arbitration agreements that would prevent ERISA Section 502(a)(2) claims that seek statutory plan-wide relief

---

dence was to be mailed to their current address on file and PIN changes and resets are always mailed to the permanent address on file. The Tenth Circuit affirmed that decision, holding that the plan administrator's decision to not reimburse the plaintiff for the amount the plaintiff's ex-wife withdrew was not an abuse of discretion. The Tenth Circuit instead found that the plan administrator safeguarded plan assets as they had already been paid out in the plaintiff's name and to do so again then depletes plan assets. Based on the court's ruling in *Foster*, which rested heavily on the facts of that case, a plan may not be liable to a participant under ERISA Section 502(a)(1)(B) for denial of benefits where the plan follows procedures that are communicated to participants and where participants are found not to have followed those procedures.

[28] See e.g., Giannini v. Transamerica Retirement Solutions, Case No. 7:21-cv-10282 (December 2, 2021, S.D.N.Y.) for an action brought by a retirement plan participant against a third party recordkeeper after notification of data breach exposing personally identifiable information asserting claims such as negligence, breach of contract and non-ERISA breach of fiduciary duty for failure to exercise reasonable care in securing and safeguarding personally identifiable information; this case was later withdrawn.

[29] See LaRue v. DeWolff, Boberg & Associates, Inc. 552 U.S. 248 (2008).

[30] See Dorman v. Charles Schwab Corp., 780 F. App'x 510, 514 (9th Cir., 2019). The Ninth Circuit Court of Appeals upheld the enforceability of an arbitration and class action-waiver provision in an ERISA governed defined contribution retirement plan, which precluded the plan participants from pursuing a class action case for breach of fiduciary duties under ERISA.

for plan wide losses.[31] Under the "effective vindication" doctrine,[32] arbitration provisions cannot operate as a prospective waiver of a party's right to pursue statutory remedies. Thus, the enforceability of arbitration provisions in plan documents is not guaranteed. Although there can be many pros and cons when weighing the costs between defending class action litigation versus arbitration of plan cybersecurity breach cases, one drawback of individual arbitration in this context is having to undergo a series of arbitrations with multiple plan participants, if not all, depending on the scope of a cybersecurity incident creating precedent that plaintiffs can use in subsequent arbitration proceedings.

§ 6.06 CONCLUDING THOUGHTS

While a few years ago it may have seemed as though undertaking a project related to establishing or evaluating procedures for cybersecurity for employee benefit plan data could wait, that is no longer the case. Even though this topic requires navigation of complex issues, knowledge of cybersecurity protections and vulnerability risks is more widely-held which makes tackling this task less intimidating. Given the fact that cybersecurity breach incidents are more frequent, litigation is evolving, and American workers data and benefit accounts are at risk, it is time for plan sponsors and fiduciaries, organizational leadership and their cybersecurity professionals, and third party service providers to work in tandem to address these issues. Technology and AI will continue to evolve, cybersecurity risk will endure, cybersecurity breach cases will continue to emerge, and security measures will continue to require updates and enhancements. It will remain crucial for plan sponsors and fiduciaries to monitor plan cybersecurity practices internally within their organization and externally among service providers periodically during the plan year, promptly address any weaknesses, update protocols, educate participants on steps they should take to protect their personal data and accounts, and for all parties to remain vigilant.

---

[31] See e.g., Harrison v. Envision Mgmt. Holding, Inc. Bd. Of Dirs., 59 F 4th 1090 (10th Cir. 2023).

[32] See Am. Express Co. v. Italian Colors Restaurant, 570 U.S. 228, 235 (2013); Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614 (1985).