Data Breach and Cybersecurity Issues in ERISA Benefits Plans



Presented by:

Daniel B. Garrie Esq., Co-Founder and Senior Managing Partner, Law & Forensics, Neutral, Mediator, E-discovery Special Master, JAMS

George Pierce, Director Emeritus and Special Legal Counsel, Toyota Tsusho America, Inc.

Melanie Phillips, Of Counsel, Orrick, Herrington & Sutcliffe LLP

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Co-founder, Law & Forensics
Mediator, Arbitrator, and
eDiscovery Special Master, JAMS



George Pierce
Director Emeritus and
Special Legal Counsel
Toyota Tsusho America,
Inc.



Melanie Phillips
Of Counsel
Orrick, Herrington & Sutcliffe
LLP

(c) 2022 Lexeprint Inc. All Rights Reserved.



Agenda

- Overview – What is ERISA?
- Considerations for Plan Sponsors and Fiduciaries
- Case Law
- Tips and Recommendations
- Key 12 Responsibilities of Plan Providers
- Key Takeaways

(c) 2022 Lexeprint Inc. All Rights Reserved.

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is ERISA?

- The **Employee Retirement Income Security Act (ERISA)** was enacted in 1974. Title 1 is part of U.S. labor laws and governs the structure of employee benefits plans.
- The Act:
  - Requires detailed disclosure to covered individuals;
  - Requires detailed reporting to the government;
  - Imposes strict fiduciary code of conduct on those who sponsor and administer ERISA Plans.; and
  - Imposes federal mechanism for enforcing rights and duties with respect to ERISA Plans and preempts a large body of state laws.

(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-ND



ERISA Plan Elements

ERISA Plans should:

- provide participants with access to plan features and funding;
- establish minimum standards for ERISA involvement by the employer;
- allow benefit use to participants and beneficiaries.

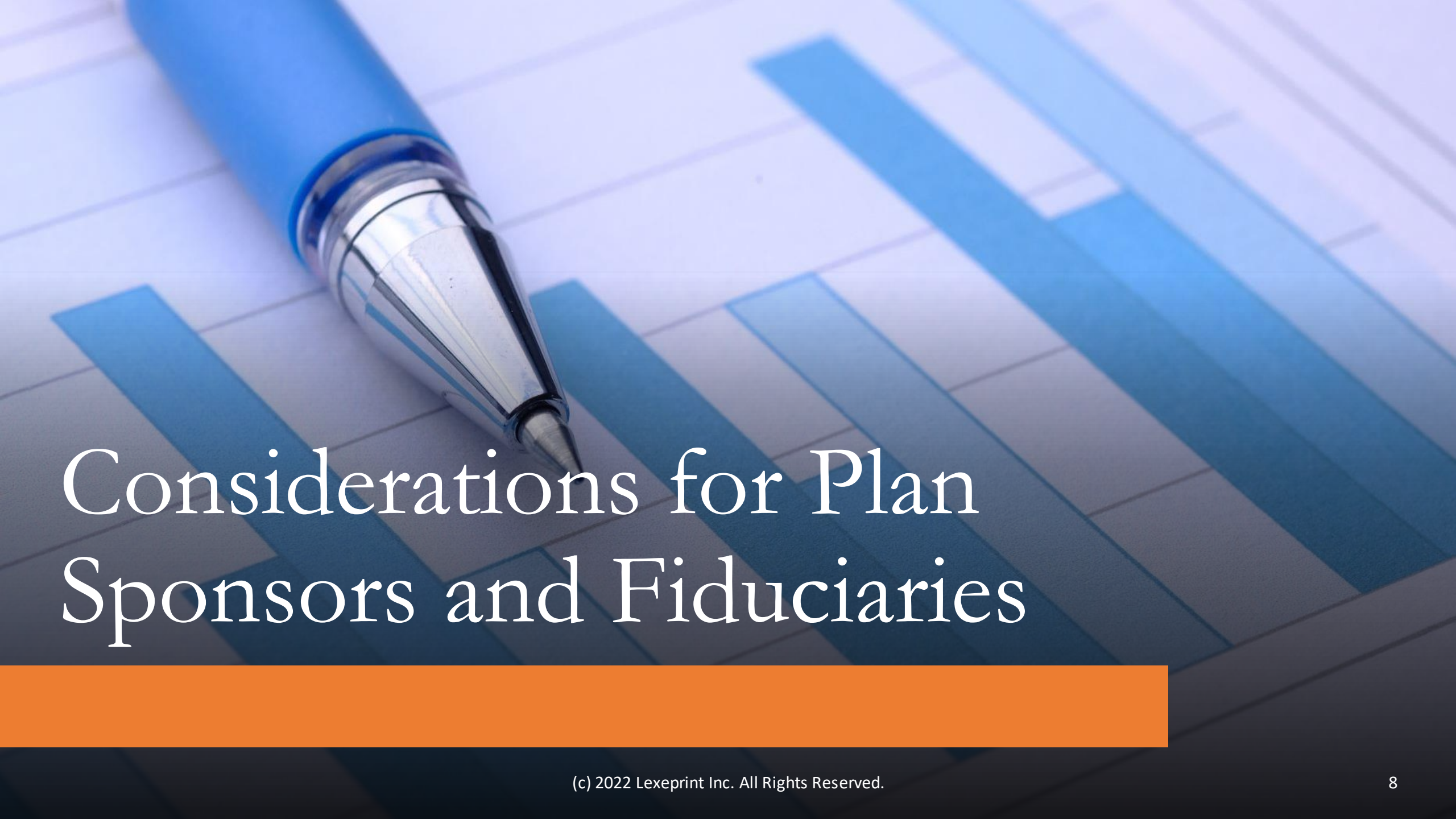
(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of Cybersecurity Issues and ERISA

- There are new cybersecurity developments and observations. These include those relating to the U.S. Department of Labor's (DOL) review of cybersecurity issues.
- These recent developments and observations must be considered by plan sponsors and other fiduciaries of employee benefit plans subject to ERISA.
- Plan sponsors and fiduciaries should be aware of the following concerns.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Considerations for Plan Sponsors and Fiduciaries

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

U.S. Department of Labor Cybersecurity Guidance

- On April 14, 2021, the DOL issues a framework to mitigate cyber breaches against ERISA.
- The plan was release in three parts:
  - Tips for Hiring a Service Provider with Strong Cybersecurity Practices,
  - Cybersecurity Program Best Practices, and
  - Online Security Tips.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Tips for Hiring a Service Provider with Strong Cybersecurity Practices

- The first section of the plan recommends:
  - Comparing service provider's cyber reputation, "security standards, practices and policies and audit results to standards adopted by other financial institutions;"
  - Establishing "contractual provisions that give the plan the right to review audit results;" and
  - Evaluating "prior security breaches and its response to those breaches." *ABA

(c) 2022 Lexeprint Inc. All Rights Reserved.



Cybersecurity Program Best Practices

- The second section of the plan recommends:
  - Administrating annual risk assessments;
  - Ensuring the cybersecurity program is updated annually; and
  - Conduct "routine data backup, patch management, and periodic cybersecurity awareness training." *ABA

(c) 2022 Lexeprint Inc. All Rights Reserved.



Online Security Tips

- The third section of the plan recommends:
  - Establishing a routine monitoring plan;
  - Encourage the use of complex passwords and multi-factor authentication; and
  - Update personal contact information.

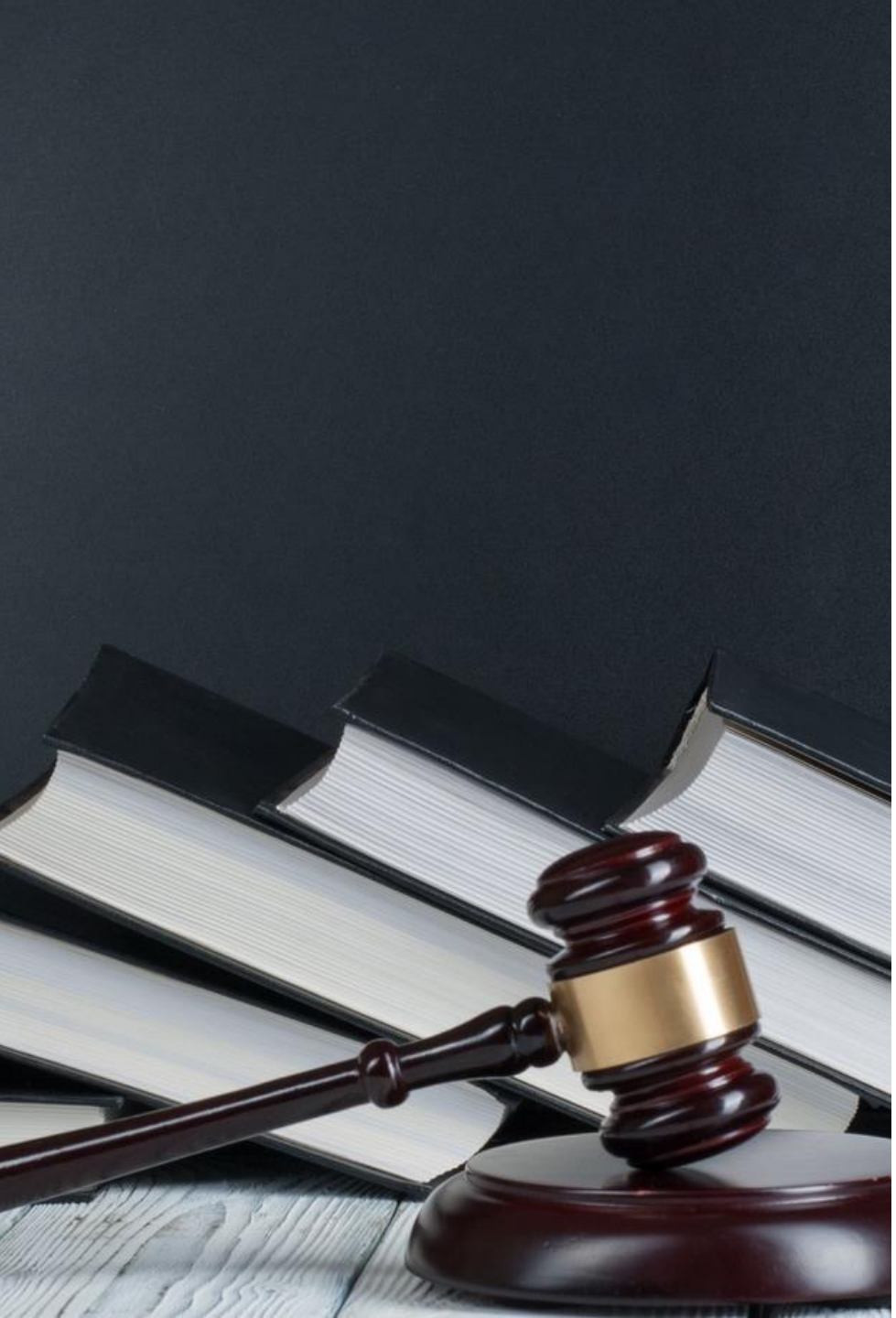
(c) 2022 Lexeprint Inc. All Rights Reserved.

Case Law



(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-ND



Disberry v. Employee Relations Committee of the Colgate-Palmolive Co. et al.

- Facts: Paula Disberry began to participate in the company 401(k) plan in 1998 and alleges that Alight Solutions and the Bank of New York Mellon "breached their duties under ERISA by allowing an unauthorized distribution from her account." Disberry claims that $750,000 in value was drained from her account. *Disberry v. Employee Relations Committee of the Colgate-Palmolive Co. et al., case number 1:22-cv-05778 * Disberry seeks relief in the form of restored plan losses and investment earnings, as well as attorney fees and costs.
- Observation:
  - The case is significant since it is one of the first cases to avoid settling.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Martin Walsh v. Alight Solutions LLC

- Facts: In July 2019, the Department of Labor began to investigate Alight Solutions to determine whether the company engaged in any ERISA violations. After the DOL concluded that Alight had violated its service provider agreements, the DOL also found that the company failed to report cybersecurity breaches and related unauthorized distributions in a timely manner.
- Observation:
  - The case underscores the DOL's authority to investigate and ensure cybersecurity breaches are properly addressed to protect benefit plans.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Giannini v. Transamerica Retirement Solutions LLC

- Facts: Eric Giannini sued Transamerica on the basis that he was a victim of identity theft after his personal information was stolen. Moreover, Giannini alleges the company violated state consumer protection and security laws in California and New York after claims against Transamerica included "negligence, breach of contract and unjust enrichment."
- Observation:
  - Although the plaintiff does not seek relief under ERISA, the case demonstrates that cyber attacks on 401(k) accounts have become prominent and companies can be held liable for their mishaps.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Tips and Recommendations

(c) 2022 Lexeprint Inc. All Rights Reserved.



#1 Request for a cybersecurity policy

- A request for a cybersecurity policy is now included in the DOL's standard document request list for benefit plan reviews.
- It is improbable that a plan will receive a closing letter from the DOL without producing an existing or adopting a new cybersecurity policy.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Recommendations

- Adopt a cybersecurity policy that is applicable to all benefit plans subject to ERISA.
- For example:
  - A stand-alone policy document specified to the ERISA benefit plans; or
  - Include into any existing corporate cybersecurity policies. Also, keeping in mind that there may need to be some revision to fully address the DOL's cybersecurity guidance.

(c) 2022 Lexeprint Inc. All Rights Reserved.



#2 Increased cyberattacks against benefit plans

- Cyber criminals have increasingly attacked benefit plans as they are seen as lucrative targets, considering that there is almost "$9.3 trillion in plan assets held in retirement accounts systemwide and the treasure trove of participant data maintained in online databases by plan sponsors, plan fiduciaries, third-party administrators, and recordkeepers for all plan types."
- The increased electronic access to benefit portals by participants has also contributed to a large number of cyberattacks per month.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA.

Recommendations

- Adhere to a widely accepted cybersecurity framework
  - ERISA is aligned with NIST CSF.
- Initiate a cybersecurity review.
- Implement an ongoing testing program to monitor information and administrative systems to promptly remedy gaps that could potentially lead to a cybersecurity breach if not quickly addressed.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC.

#3 Vendor Services Agreements may not adequately protect against the risk of cybersecurity issues

- Considering how recent the DOL's cybersecurity guidance is, many vendor services agreements entered by plan sponsors regarding their benefit plans would not adequately protect them from DOL-specific cybersecurity risks.
- Unless these agreements specifically implicate HIPAA and specifically address cybersecurity issues in related Business Associate Agreements, vendor services agreements that do not specifically obligate vendors compliance with the DOL's cybersecurity guidance may limit liability and indemnity provisions or related breach of contract claims.

(c) 2022 Lexeprint Inc. All Rights Reserved.



#3 Vendor Services Agreements may not adequately protect against the risk of cybersecurity issues

- Vendor service agreements do not usually provide for special and/or consequential damages.
- So, a general compliance with laws representation may not suffice as a hook for indemnification purposes in the instance of a cybersecurity breach because breach-related damages are usually considered special and/or consequential.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

Recommendations

- Review existing vendor services agreements and consider renegotiating the terms of these agreements to include cybersecurity representations and other terms; or
- Consider waiting until and upcoming renewal to negotiate the addition of a data privacy and security addendum until appropriate cybersecurity terms can be included into the main agreement as part of the renewal negotiations.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC-ND.

#4 Current Cybersecurity Liability Insurance policies may not cover breaches involving benefit plans

- Policies that list the plan sponsor as the insured party may not cover cybersecurity breaches affecting benefit plans or plan fiduciaries.
- If plan sponsors or fiduciaries have failed to implement adequate controls and safeguards to protect benefit plan assets and participant against common cybersecurity threats or have failed to conduct required tabletop exercises to ensure such safeguards are adequate, cybersecurity liability insurers may use this as an argument against covering damages that may arise out of a breach.

(c) 2022 Lexeprint Inc. All Rights Reserved.



#4 Update Cybersecurity Awareness Training

- Must be conducted at least annually for all personnel.
- It should be updated to reflect issues identified in the most recent risk assessment.
- Goal is to educate everyone on current threats, help prevent incidents, and respond to a potential threat.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Recommendations

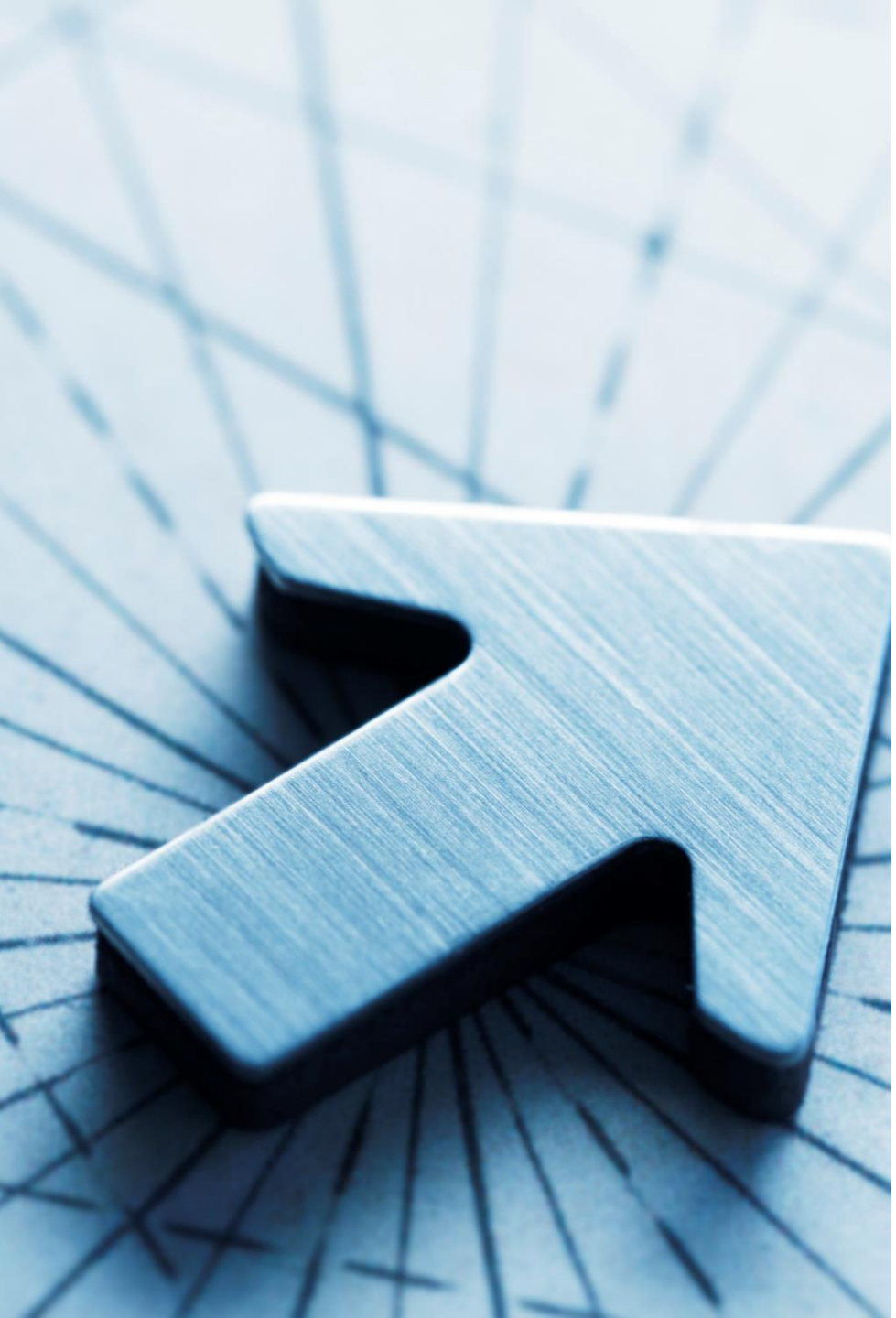
- Review existing cybersecurity liability insurance policies to confirm whether their benefit plans, plan fiduciaries and plan sponsors are covered in the event of a breach.
- Review policy compliance requirements.
- Consider obtaining additional cybersecurity liability coverage.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Key 12 Responsibilities of Plan Providers

(c) 2022 Lexeprint Inc. All Rights Reserved.



Responsibilities of Plan Providers with DOL Guidance

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure 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.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Responsibilities of Plan Providers

7. Conduct periodic cybersecurity awareness training.

8. Implement and manage a secure system development life cycle (SDLC) program.

9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

10. Encrypt sensitive data, stored and in transit.

11. Implement strong technical controls in accordance with best security practices.

12. Appropriately respond to any past cybersecurity incidents.

(c) 2022 Lexeprint Inc. All Rights Reserved.



#1 Formal, Well Documented Cybersecurity Program

- A strong cybersecurity program will identify and assess internal and external cybersecurity risks that may threaten the confidentiality, integrity or availability of stored nonpublic information.
- Well- documented information security policies, procedures, guidelines and standards should be fully implemented to protect the security of the IT infrastructure and data stored on the system.

(c) 2022 Lexeprint Inc. All Rights Reserved.



#2 Conduct Annual Risk Assessments

- Risk Assessments identify, estimate and prioritize information system risks.
- Cyber and IT threats are ever-changing, so it is essential that companies design a practicable, effective risk assessment schedule.

(c) 2022 Lexeprint Inc. All Rights Reserved.

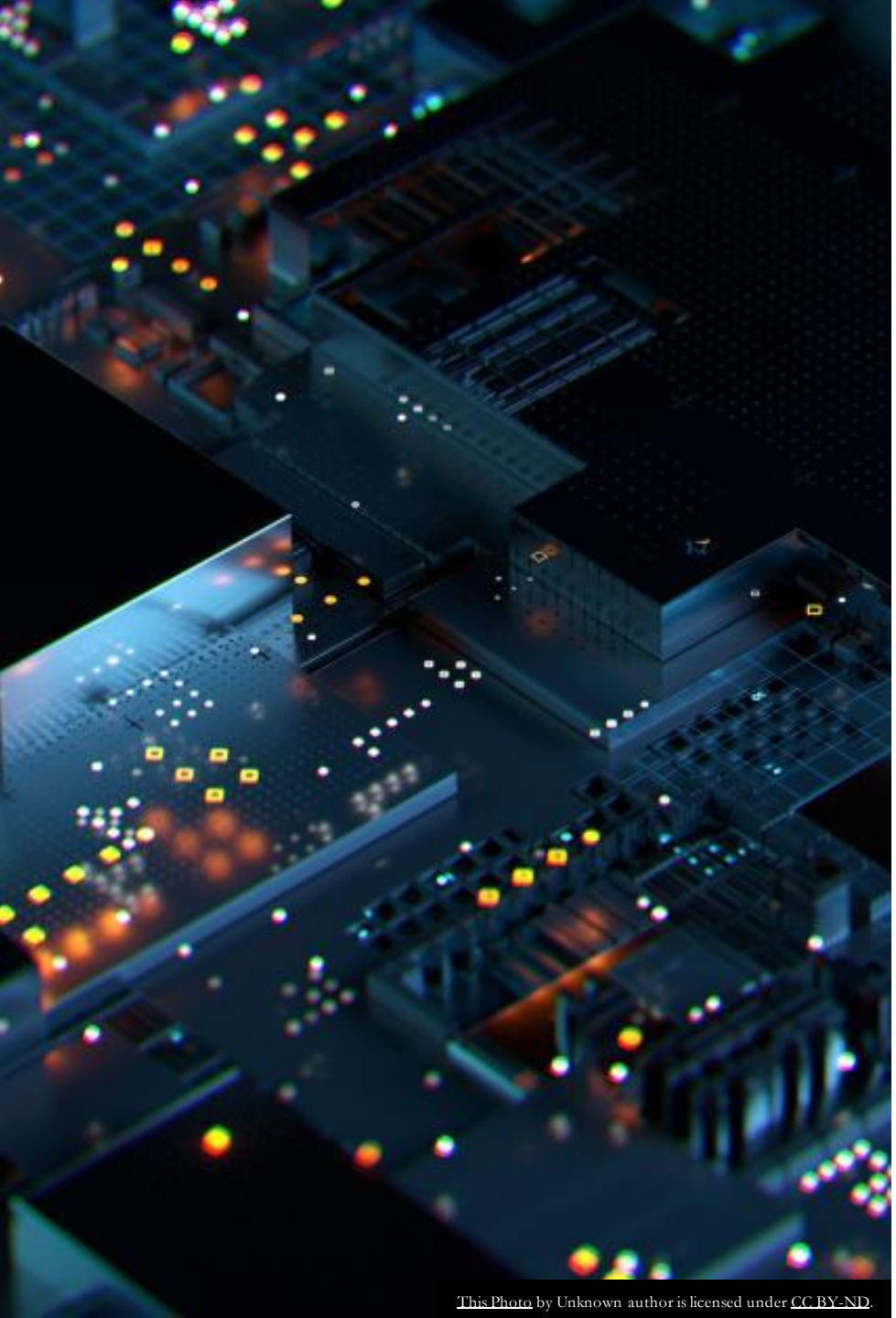


This Photo by Unknown Author is licensed under CC BY

#3 Annually Audit Security Controls

- Using a third-party auditor to assess your company's security controls will allow for a clear, unbiased report that includes the existing risks, vulnerabilities and weaknesses.

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-ND.

#4 Define and Assign Information Security Roles and Responsibilities

- A cybersecurity program should be managed by the senior executive level (the CISO).
- Usually, a CISO will establish and maintain the strategy and overall operation of the cybersecurity program which is being performed by sufficiently qualified personnel.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

#5 Ensure strong Access Control Procedures

- Access Control is a method of guaranteeing that users are who they say they are. This method ensures that the individual has the appropriate access to IT systems and data.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-ND.

#5 Ensure strong Access Control Procedures

- Some best security practices for access controls are:
  - "Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.
  - Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.
  - Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.
  - All employees use unique, complex passwords."

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY.

#6 Security Reviews and Independent Security Assessments

- Assets/Data stored in a Cloud or managed by a third-party Service Provider are subject to suitable security review and independent security assessments.
- Cloud computing raises many unique security issues and challenges. So, companies must understand the security posture of the cloud service provider.
- Understanding how the cloud service provider security controls operate will allow for sound decisions to be made using the service.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

#7 All personnel undertake an annual Cybersecurity Awareness Training

- All personnel should participate in an annual cybersecurity awareness training and should be kept up-to-date about the growing cyber risks and mitigating strategies.
- A robust cybersecurity awareness program will set clear cybersecurity expectations for all employees and educate them as to potential attack vectors, assist in preventing cyber-related incidents and responding tactics to a potential threat.

(c) 2022 Lexeprint Inc. All Rights Reserved.



#8 Secure System Development Life Cycle Program (SLDC)

- A strong SLDC process ensures that security assurance activities (pen testing, code review, architecture analysis) are a part of the system development effort.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

#9 Business Resiliency Program

- Business resilience refers to a company's ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and data.
- This program can include a Business Continuity Plan, Disaster Recovery Plan and Incident Response Plan.

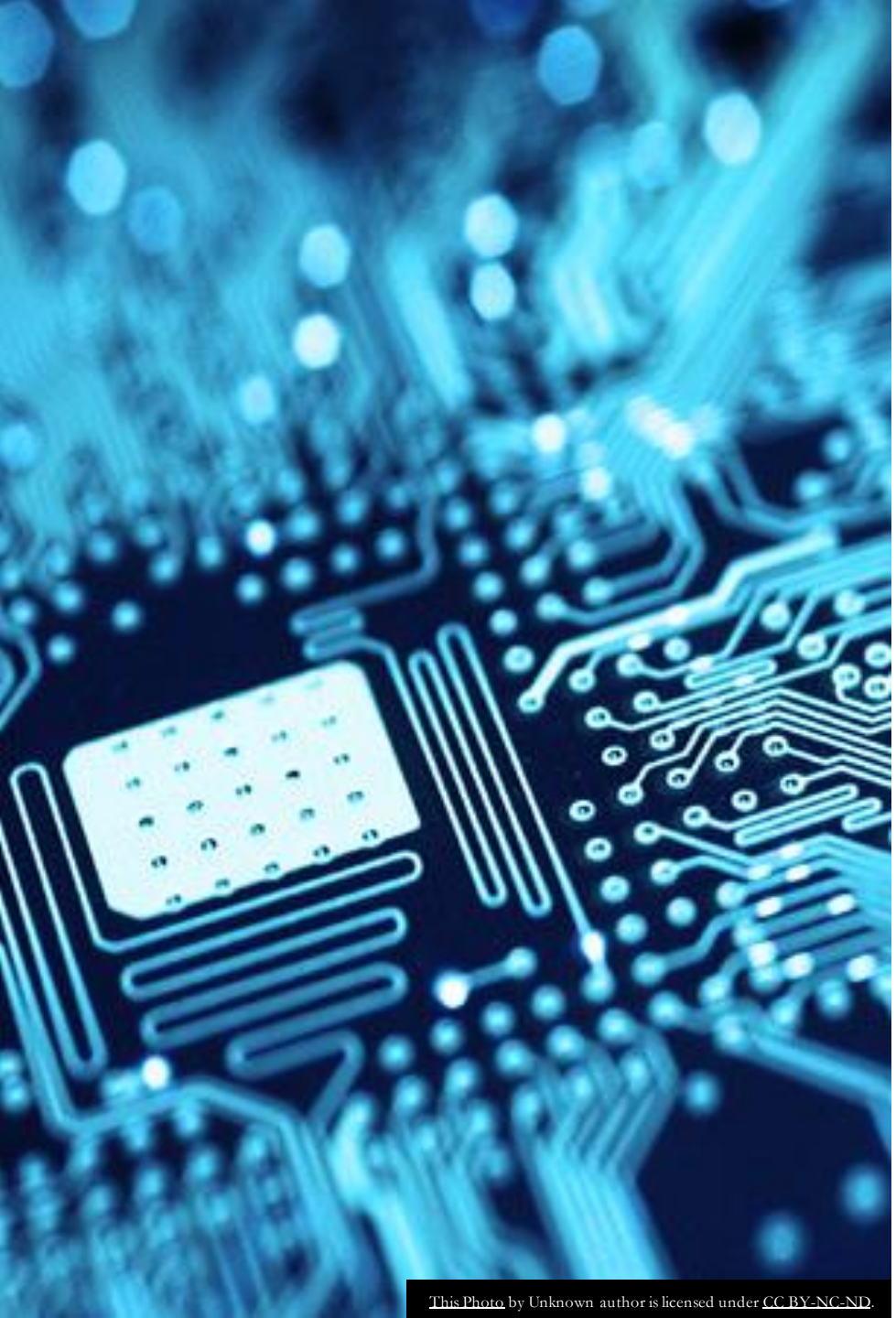
(c) 2022 Lexeprint Inc. All Rights Reserved.



#10 Encryption

- Data Encryption is an essential part of security for sensitive data and data in transit.
- Best practices include implementing:
  - Current standards for encryption keys,
  - Message authentication, and
  - Hashing.

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC-ND.

#11 Implement Technical Controls that follow Best Security Practices

- The information system implements technical security solutions through different mechanisms included in the hardware, software or firmware components of the system.
- Best security practices for technical security includes:
  - Network segregation,
  - System hardening, and
  - Current and regular update of antivirus software.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC.

12 Appropriate and timely action to Cybersecurity Incidents or Breaches

- Appropriate action should be taken once a cybersecurity breach or incident has been identified.
- Suitable action should be taken to protect the plan and its participants. This includes:
  - Informing law enforcement,
  - Notifying the appropriate insurer, and
  - Investigation of the incident, etc.

(c) 2022 Lexeprint Inc. All Rights Reserved.

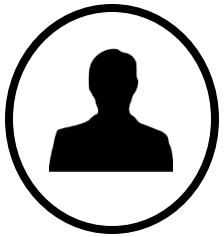
Key Takeaways

Weigh	Weigh the recommendations against your existing cybersecurity programs and safeguards to determine what would be the most appropriate response.
Evaluate	Evaluate and appropriately respond to the DOL's cybersecurity guidance and related issues.
Do NOT wait	Do NOT wait until ERISA benefit plans become a victim of a cybersecurity attack!

(c) 2022 Lexeprint Inc. All Rights Reserved.


Questions?

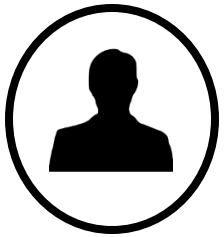
Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



Melanie Phillips
Email: mphillips@orrick.com
URL: https://www.orrick.com/



George Pierce
Email: george_pierce@taiamerica.com

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics LLC – Co-Founder
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybers ecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engin eering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He an d his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been aw arded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack. IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme C ourt Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved.



George Pierce
Toyota Tsusho America, Inc. - Director Emeritus and Special Legal Counsel
Contact:
E: george_pierce@taiamerica.com

TOYOTA TSUSHO AMERICA, INC.

Mr. Pierce joined Toyota Tsusho America in 1993 and established the company's Legal Department. He advises on cyber security, legal and regulatory compliance matters concerning the company's operations in the United States, Canada, and Mexico. He has continuously served on Toyota Tsusho America's board of directors from 2000 until 2022 and is currently a director emeritus. He has also served on the boards of directors of several subsidiary companies.

Before joining Toyota Tsusho America, Mr. Pierce was associated with Mudge Rose Guthrie Alexander and Ferdon where he had extensive experience in various litigation matters including environmental insurance coverage, white collar defense, internal investigations, and trade and regulatory compliance.

Mr. Pierce was admitted to the bar of the State of New York in 1982 and has spoken on cyber security matters at various webinars, and on labor and employment issues at meetings of the American Bar Association, the International Section of the New York State Bar Association and the International Bar Association, as well as the Practicing Law Institute, the American Chamber of Commerce in Japan, the Japanese Chamber of Commerce and Industry of New York, and the Japan Society. He received his law degree from the University of Denver College of Law in 1981. He also holds a master's degree in Sociology from the University of Northern Colorado and a bachelor's degree with majors in Psychology and Japanese Language from the University of Colorado, Boulder.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Melanie Phillips
Of Counsel – Orrick, Herrington & Sutcliffe LLP
Contact:
W: (206) 839-4323
E: mphillips@orrick.com
URL: https://www.orrick.com/

Melanie Phillips works with clients to create practical solutions for their data collection, management, and security practices.

Melanie advises clients in various critical areas, including incident response planning, incident response, consumer breach litigation, and regulatory enforcement actions. She has worked on cybersecurity incident and data breach investigations for a range of clients, including enterprise-wide network intrusions. Melanie also assists clients with digital crime investigations. With more than a decade of litigation experience, including in key areas of trade secret, employment, and consumer protection matters, she has a holistic understanding of the key drivers of privacy and security in organizations big and small.

Melanie has dedicated countless hours to pro bono work over her career, focused on issues relating to domestic violence. She was awarded the Honorable Benjamin Aranda III Outstanding Public Service Award in 2014 in recognition of her work with the Los Angeles County Bar Association Domestic Violence Clinic. She also earned the Pro Bono Award at Orrick for her outstanding commitment to pro bono work in 2007 relating a complicated VAWA petition on behalf of an Iraqi interpreter working for the United States military.

2022 Cybersecurity Issues and Recommendations for ERISA Plan Fiduciaries

02.01.2022 | UPDATES

New cybersecurity developments and observations, including those relating to U.S. Department of Labor's (DOL) review of cybersecurity issues, warrant prompt consideration by plan sponsors and other fiduciaries of employee benefit plans subject to ERISA.

In our April 2021 update, we reported on the DOL's long-anticipated cybersecurity guidance applicable to both retirement and health and welfare plans. Though group health plan sponsors may be familiar with similar cybersecurity requirements imposed under HIPAA, the DOL's cybersecurity guidance (in the form of "best practices" and "tips") raise new considerations for retirement plans as well as welfare plans. These considerations are in addition to HIPAA data security requirements applicable to group health plans. Plan sponsors and fiduciaries should be attentive to the following concerns:

1. **The DOL's standard document request list for benefit plan reviews now includes a request for a cybersecurity policy.** It appears unlikely that a plan will receive a closing letter from the DOL without producing an existing or adopting a new cybersecurity policy. This has been our experience to date, even though plan sponsors and fiduciaries can take the position that the DOL's cybersecurity guidance is framed as an agency recommendation of best practices and that a cybersecurity policy is not required by ERISA.

   Recommendation: Consider adopting a cybersecurity policy applicable to all benefit plans subject to ERISA (i.e., within the purview of the DOL's investigative authority). This cybersecurity policy can take the form of a standalone policy document specific to the ERISA benefit plans or it may be addressed in existing corporate cybersecurity policies (noting that some revision may be needed to fully address the DOL's cybersecurity guidance).

2. **Benefit plans are increasingly being targeted by cyberattacks.** Benefit plans are increasingly viewed as lucrative targets for cyber criminals, given the almost $9.3 trillion in plan assets held in retirement accounts systemwide and the treasure trove of participant data maintained in online databases by plan sponsors, plan fiduciaries, third-party administrators, and recordkeepers for all plan types. Further, increased electronic access to benefit portals by participants using internet-connected devices, including cell phones, laptops, and tablets, which suffer an average of 5,200 cyberattacks per month, makes it easier for bad actors to improperly access such benefit plan systems. Because it is a matter of not if—but when—a benefit plan will experience a cyberattack, plan sponsors and fiduciaries should be motivated to act promptly to implement the DOL's guidance despite its being framed as best practices.

   Recommendation: Consider initiating a cybersecurity review and ongoing testing program to monitor their information and administrative systems and promptly remedy gaps that could lead to a cybersecurity breach if not addressed.

3. **Existing vendor services agreements may not sufficiently protect plan sponsors against the risk of cybersecurity issues.** Given the recency of the DOL's cybersecurity guidance, it is likely that many vendor services agreements entered into by plan sponsors with respect to their benefit plans do not adequately protect sponsors from DOL-specific cybersecurity risks. Except for those agreements specifically implicating HIPAA and specifically addressing cybersecurity issues in related Business Associate Agreements, vendor services agreements that do not specifically obligate vendors compliance with the DOL's cybersecurity guidance may limit liability and indemnity provisions, or related breach of contract claims, contained in the agreements in the event of a cybersecurity breach. Further, because vendor services agreements often carve out special and/or consequential damages, a general compliance with laws representation may not serve as a hook for indemnification purposes in the event of a cybersecurity breach, as breach-related damages are often considered special and/or consequential.

   Recommendation: Consider reviewing existing vendor services agreements and either renegotiate the terms of such agreements to include cybersecurity representations and other terms (specifically referencing the DOL's cybersecurity guidance) or, if the preference is to wait until an upcoming renewal, negotiate the addition of a data privacy and security addendum until appropriate cybersecurity terms can be incorporated into the main agreement as part of renewal negotiations.

4. **Existing cybersecurity liability insurance policies may not cover breaches involving benefit plans.** Plan sponsors often procure either standalone cybersecurity liability insurance policies or riders to broader commercial liability coverage. However, policies that list the plan sponsor as the insured party might not cover cybersecurity breaches affecting benefit plans or plan fiduciaries, even if the plan sponsor is financially responsible for related damages. Further, cybersecurity liability insurers may have another argument against covering damages arising out of a breach if the plan sponsor or fiduciary has failed to implement adequate controls and safeguards to protect benefit plan assets and participant data against common cybersecurity threats, or has failed to conduct required tabletop exercises ensuring such safeguards are adequate.

   Recommendation: Consider reviewing existing cybersecurity liability insurance policies to confirm whether their benefit plans and plan fiduciaries, in addition to plan sponsors, would be covered in the event of a breach, and review policy compliance requirements. If not, we recommend that plan sponsors considering procuring additional, appropriate cybersecurity liability coverage.

The above recommendations are general considerations for plan sponsors and fiduciaries, which will need to be weighed against existing cybersecurity programs and safeguards to arrive at appropriate responses. While strategy will vary, it is important that plan sponsors and fiduciaries evaluate and appropriately respond to the DOL's cybersecurity guidance and related issues proactively and not wait until applicable ERISA benefit plans become the victim of a cybersecurity breach or the subject of a DOL review.

© 2022 Perkins Coie LLP

CONTACTS

April Goff
Kiran H. Griffith
Kurt E. Linsenmayer
Jeff Minzel
Tomer Vandsburger

RELATED SERVICES

PRACTICES

- Employee Benefits & Executive Compensation
- Labor & Employment Law
- Privacy & Security Law
- Corporate & Securities
- Corporate Finance
- Public Companies
- Capital Markets

RELATED NEWS & INSIGHT

UPDATES

04.22.2021
US Department of Labor Issues Highly Anticipated Cybersecurity Guidance for ERISA Plans

© 2022 Perkins Coie LLP

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Cybersecurity Breach Suits Benefits Lawyers Should Watch

By **Kellie Mejdrich**

Law360 (July 22, 2022, 7:48 PM EDT) -- Attempts to steal workers' personal information and even their retirement savings are on the rise, attorneys say, raising questions about plans' and third-party administrators' exposure for cybersecurity breaches under federal benefits law.

Earlier this month, a retiree sued her former employer Colgate-Palmolive under the Employee Retirement Income Security Act, alleging plan fiduciaries breached their duties by failing to prevent a fraudster from hijacking her 401(k) account.

In addition to that suit, benefits lawyers say they are keeping an eye on large class actions pending in New York and Georgia against third-party plan administrators claiming injury over leaked personal information.

The U.S. Government Accountability Office in a February 2021 report warned about increased legal risks to ERISA plan fiduciaries stemming from cyber breaches, pointing to recent lawsuits alleging that cyberattacks resulted in unauthorized distributions from retirement plan accounts.

The GAO warned in its report that outsourcing retirement plan administration to third parties — something increasingly common for many employers — could boost opportunities for malicious individuals to gain unauthorized access.

Bailey & Glasser LLP partner Mark G. Boyko said that ERISA could prove to be a potent tool for plaintiffs in this burgeoning field of litigation.

"I just think this is going to be a growing area. I think it's only a matter of time before there are larger-scale successful hacks that actually succeed in removing large amounts of participant assets from a plan," he said. "In that situation, I think that ERISA is going to be probably the strongest tool that the participants have to protect themselves from that."

Here are four cases that could shed light on companies' responsibilities when it comes to protecting retirement plan participants from online intruders.

Colgate-Palmolive Plan Sued Over Drained 401(k)

Paula Disberry, a retired Colgate-Palmolive marketing executive, sued her former employer and other companies involved with her 401(k) retirement plan on July 7 in New York federal court, seeking to recoup losses after a thief took over her account and drained it of more than $750,000 in value.

The case is significant for benefits attorneys because similar challenges brought by individuals under ERISA seeking to restore plan assets resulting from cyber intrusions have settled. Significant settlements included a closely watched 2020 challenge brought against Abbott Laboratories as well as a 2019 suit against Estee Lauder Inc., each from individual retirees alleging plan fiduciaries breached their ERISA duties by allowing unauthorized distributions from their accounts.

Disberry, a South African resident who first became eligible to participate in the company 401(k) plan in 1998, alleges the company's employee relations committee, benefits administration company Alight Solutions and plan trustee The Bank of New York Mellon were fiduciaries of the plan and breached their duties under ERISA by allowing an unauthorized distribution from her account.

Disberry said in the complaint she learned in September 2020 that her account had been drained of its entire balance in a single taxable lump sum in March of that year. A fraudster in Las Vegas was the culprit, Disberry said, who had contacted Alight in January 2020, falsely impersonated her and requested the company mail a temporary personal identification number to her address in South Africa. The fraudster ultimately intercepted that mail and used the PIN to take over her retirement account credentials, later mailing the plan distribution to a newly added Las Vegas address.

Disberry seeks relief in the form of restored plan losses and investment earnings, as well as attorney fees and costs.

"We feel confident that the ERISA claims will stick," said Kirsten Scott, partner with Renaker Hasselman Scott LLP and attorney for Disberry.

"Each of the defendants that we've named in the case exercised authority or control with respect to the management of or disposition of plan assets, or they had discretionary responsibility in administering the pension plan," Scott said.

Elliot D. Raff, member at McDonald Hopkins LLC, said issues in the Disberry case demonstrate the range of liability faced by employers and other companies involved in benefit plan administration.

"Employers need to be thinking about, what kind of ERISA fiduciary record have they made? Because if I'm Mrs. Disberry, I'm suing everybody," Raff said.

The case is Disberry v. Employee Relations Committee of the Colgate-Palmolive Co. et al., case number 1:22-cv-05778, in the U.S. District Court for the Southern District of New York.

DOL Authority Challenge Pending

The Seventh Circuit could soon rule on a challenge brought by Alight Solutions to the U.S. Department of Labor's authority to investigate cybersecurity breaches, after a three-judge panel heard oral **arguments in April** in the company's appeal of a court-ordered subpoena in a cybersecurity-focused investigation.

The DOL first requested information from Alight in 2019, which provides record-keeping and administrative services for more than 750 employee benefit plans serving around 20.3 million people, as part of an investigation into whether cybersecurity breaches resulted in unauthorized distributions from ERISA plan accounts.

Alight appealed to the Seventh Circuit in December after the DOL obtained a subpoena enforcement order for the information in Illinois federal court, arguing that cybersecurity — and investigating Alight for nonfiduciary acts — fell outside the scope of the DOL's authority under ERISA. Alight asked the circuit panel to overturn the subpoena, which the district court refused to stay pending the appeal.

Earlier this month, a federal magistrate judge in Illinois overseeing the district case **approved a protective order** limiting how federal agencies can share information obtained in the DOL's investigation.

Ivelisse Berio LeBeau, partner with the Wagner Law Group, said she's keeping a close eye on the appeal.

"I think it underscores the DOL's authority to investigate, regarding cybersecurity breaches and benefit plans," Berio LeBeau said.

"I think the guidance last year that was issued was a sign that they're interested. The [Employment Benefits Security Administration] has made no secret that they are concerned. Because, frankly, there's a whole lot of personally identifying information and a whole lot of assets related to employee benefit plans," Berio LeBeau said.

The case is Martin Walsh v. Alight Solutions LLC, case number 21-3290, in the U.S. Court of Appeals for the Seventh Circuit.

Workers Target 401(k) Record-keepers

Employee 401(k) plan participant Eric Giannini seeks to represent thousands in a proposed class action after benefits administration company Transamerica Retirement Solutions notified him that his personal data was stolen in a 2021 cybersecurity breach.

Giannini first sued in New York federal court in December on behalf of "individual retirement fund plan participants who used Transamerica's services and had their sensitive [personally identifying information] accessed by unauthorized parties because of a lapse in network security in or around June of 2021." He alleged he was a victim of identity theft after hackers stole his personal information including his address, Social Security number, figures related to retirement plan distributions, and tax information.

Giannini's complaint largely asserts state tort claims and doesn't seek relief under ERISA, which is typical of many cases involving personal information obtained through employee benefit plan administrators.

Giannini alleged he already experienced fraudulent purchase requests and spam calls, but alleged he and other class members would experience "a slew of harms" in the future resulting from the breach, including fraudulent charges and targeted advertising without their consent.

Claims alleged against the company include negligence, breach of contract and unjust enrichment. The complaint also alleges the security lapses violated numerous state consumer protection and data security laws including in California and New York.

Giannini seeks more than $5 million in damages as well as an injunction against the company prohibiting it from misusing private information and requiring it to issue prompt, complete and accurate disclosures; changes in the company's cybersecurity policies; and a minimum of three years of credit monitoring services for affected class members.

Raff of McDonald Hopkins said cases like the one brought by Giannini show the high risks facing plan record-keepers.

"They're in a bind, because they are spending hundreds upon hundreds of millions of dollars a year for artificial intelligence systems ... systems after systems after systems to flag and identify potential cyber crooks," Raff said of record-keepers. "And yet the cyber folks are always a step ahead, because there's money to be had."

Raff said he's learned from conversations with big record-keeping firms that hackers often target a company with sets of records that can include thousands of employees.

"They have learned how to program multiple network computers to take those data sets and throw it at the big record-keepers," he said, with many of those accounts often password-protected with phrases or keywords that might be easily guessed.

"So, the cyber thieves have come to understand that it doesn't take a lot of data to steal someone's 401(k) account and have a good chance at a big payday," he added.

The case is Giannini v. Transamerica Retirement Solutions LLC, case number 7:21-cv-10282, in the U.S. District Court for the Southern District of New York.

Workers Sue Over Massive Benefits Administration Breach

Benefit plan consulting firm Horizon Actuarial Services LLC faces a consolidated mega-class of more than 2.5 million people after a Georgia federal judge agreed in **May** to combine five class actions over a November 2021 data breach.

According to a consolidated complaint from April, the data breach resulted in the leak of sensitive information from plan participants in more than two dozen employee benefit plans, including numerous multi-employer plans.

Like the Transamerica case, the Horizon consolidated class action does not bring ERISA claims but involves employee benefit plan participants seeking legal remedies.

The cases are Sherwood v. Horizon Actuarial Services LLC, case number 1:22-cv-01495; Quan v. Horizon Actuarial Services LLC, case number 1:22-cv-01531; Bedont v. Horizon Actuarial Services LLC, case number 1:22-cv-01565; Torrano v. Horizon Actuarial Services LLC, case number 1:22-cv-01674; and Hill v. Horizon Actuarial Services LLC, case number 1:22-cv-01676, in the U.S. District Court for the Northern District of Georgia.

--Editing by Bruce Goldman.

All Content © 2003-2022, Portfolio Media, Inc.

LAW360®

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Takeaways From DOL's New Cybersecurity Guidance

By **Emily Brill**

Law360 (April 16, 2021, 7:53 PM EDT) -- The U.S. Department of Labor's first-ever guidance on employee retirement plans' cybersecurity duties set some long-awaited standards for how employers and plan administrators should protect saver data, but some questions remain about plans' legal responsibility to shield worker savings from cyberthieves.

Here, Law360 offers what benefits attorneys say are the most notable takeaways from the new guidance.

Long Time Coming

The guidance arrived April 14 courtesy of DOL's benefits unit, the Employee Benefits Security Administration, or EBSA. Tackling cybersecurity had long been on the sub-agency's to-do list, given that the ERISA Advisory Council — a committee of experts that counsels EBSA on how to administer the Employee Retirement Income Security Act — produced a report on the need for such guidance in 2016.

Last month, the Government Accountability Office added fuel to the fire, releasing a report that called on DOL to tell retirement plan sponsors how to handle cybersecurity risks. The document appeared amid a flurry of GAO reports on cybersecurity, which collectively outlined a need for the federal government to "urgently pursue critical actions to address major cybersecurity challenges" in various sectors.

"I think this was really intended to come out on the heels of that GAO report … that said we need guidance from DOL about minimum standards for cybersecurity," said Carol Buckmann, a co-founding partner of the benefits law firm Cohen & Buckmann PC. "So I was happy to see it, because we really didn't have clear guidance from the DOL. I hope that plan fiduciaries and vendors will pay careful attention to it."

Advice for Workers

EBSA's cybersecurity guidance came in three parts: one intended for employers, another for plan administrators and a third for the workers who participate in retirement plans.

Robert Projansky, the co-chair of Proskauer Rose LLP's employee benefits and executive compensation practice group, said he was pleased to see the guidance targeting plan participants, which includes tips such as "use strong and unique passwords," "keep personal contact information current" and "be wary of free Wi-Fi."

Workers' failure to follow tips like these can often leave their retirement accounts vulnerable to a cyberattack, so handing them information they can use to protect themselves is crucial, Projansky said.

"Education of participants is a key, key method of protecting plans against cyber breaches," Projansky said. "You can stop many breaches at their source by educating participants as to the importance of cybersecurity."

Advice for Employers and Plan Administrators

The guidance also includes two documents geared toward the managers of retirement plans, offering tips for employers on hiring a third-party administrator with strong cybersecurity practices and tips for TPAs on how to instate policies that protect worker data.

Dan O'Neil, an associate at Pillsbury Winthrop Shaw Pittman LLP who has written about ERISA and cybersecurity, called the documents "eminently sensible," describing their release as "a welcome development that draws attention to an under-appreciated concern in the benefits world."

The tips also shouldn't catch employers and TPAs off-guard, given that they recommend cybersecurity practices that have become commonplace.

"I think most benefits professionals, if not privacy experts themselves, are familiar with similar guardrails put in place to comply with HIPAA or state data regulations, so I think most people will recognize the concepts here — a formal plan, training, annual risk assessments, steps to take if there's a breach. These should all sound familiar at this point," O'Neil said.

Barry Salkin, an attorney at the benefits law firm The Wagner Law Group, said employers and TPAs may want to amend their contracts to address the cybersecurity practices listed in the guidance.

"From the perspective of both parties, if the DOL is saying something is a best practice, you're going to be hard-pressed to say, 'I don't need that in my contract,'" Salkin said.

Attorneys also noted that since DOL has now spelled out its cybersecurity standards for benefits plans, it's reasonable to assume these practices will be cited in ERISA lawsuits over data security and addressed in DOL audits.

Not the Last Word

Although attorneys agree the DOL didn't skimp on details in its first cybersecurity guidance, they also said the documents don't answer every question about ERISA and data security.

Some questions that remain open include: Is data about retirement plan participants a plan asset? Are employers or TPAs responsible when data breaches occur? And does ERISA preempt state cybersecurity laws, or do benefit plans have to follow those?

The questions of whether participant data is a plan asset and who bears responsibility for data breaches are currently **making their way through the courts**.

Attorneys expressed mixed feelings on whether judges or the DOL should resolve these particular issues, but most agreed that the agency's first set of guidance on ERISA cybersecurity concerns shouldn't be its last.

"I hope the DOL will go further than this, and this is only the first step in guidance that they'll be issuing, because there are a lot of issues," Buckmann said.

--Editing by Jill Coffey and Tim Ruel.

All Content © 2003-2022, Portfolio Media, Inc.

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers 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. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure 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.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate**.
- **Restore normal operations and services**.

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

- Formal and effective policies and procedures governing all the following:
  1. Data governance and classification.
  2. Access controls and identity management.
  3. Business continuity and disaster recovery.
  4. Configuration management.
  5. Asset management.
  6. Risk assessment.
  7. Data disposal.
  8. Incident response.
  9. Systems operations.
  10. Vulnerability and patch management.
  11. System, application and network security and monitoring.
  12. Systems and application development and performance.
  13. Physical security and environmental controls.
  14. Data privacy.
  15. Vendor and third party service provider management.
  16. Consistent use of multi-factor authentication.
  17. Cybersecurity awareness training, which is given to all personnel annually.
  18. Encryption to protect all sensitive information transmitted and at rest.

2. Prudent Annual Risk Assessments.

A Risk Assessment is an effort to identify, estimate, and prioritize information system risks. IT threats are constantly changing, so it is important to design a manageable, effective risk assessment schedule. Organizations should codify the risk assessment's scope, methodology, and frequency. A risk assessment should:

- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized.
- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks.
- Describe how the cybersecurity program will mitigate or accept the risks identified.
- Facilitate the revision of controls resulting from changes in technology and emerging threats.
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

3. A Reliable Annual Third Party Audit of Security Controls.

Having an independent auditor assess an organization's security controls provides a clear, unbiased report of existing risks, vulnerabilities, and weaknesses.

As part of its review of an effective audit program, EBSA would expect to see:

- Audit reports, audit files, penetration test reports and supporting documents, and any other analyses or review of the party's cybersecurity practices by a third party.
- Audits and audit reports prepared and conducted in accordance with appropriate standards.
- Documented corrections of any weaknesses identified in the independent third party analyses.

4. Clearly Defined and Assigned Information Security Roles and Responsibilities.

For a cybersecurity program to be effective, it must be managed at the senior executive level and executed by qualified personnel. As a senior executive, the Chief Information Security Officer (CISO) would generally establish and maintain the vision, strategy, and operation of the cybersecurity program which is performed by qualified personnel who should meet the following criteria:

- Sufficient experience and necessary certifications.
- Initial and periodic background checks.
- Regular updates and training to address current cybersecurity risks.
- Current knowledge of changing cybersecurity threats and countermeasures.

5. Strong Access Control Procedures.

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to IT systems and data. It mainly consists of two components: authentication and authorization. The following are best security practices for access control:

- Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.
- Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.
- Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.
- All employees use unique, complex passwords.
- Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.
- Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with, nonpublic information.
- Procedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant.
- Confirm the identity of the authorized recipient of the funds.

6. 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.

Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. Organizations must understand the security posture of the cloud service provider in order to make sound decisions on using the service.

Best practices include:

- Requiring a risk assessment of third party service providers.
- Defining minimum cybersecurity practices for third party service providers.
- Periodically assessing third party service providers based on potential risks.

- Ensuring that guidelines and contractual protections at minimum address the following:
  - » The third party service provider's access control policies and procedures including the use of multi-factor authentication.
  - » The third party service provider's encryption policies and procedures.
  - » The third party service provider's notification protocol for a cybersecurity event which directly impacts a customer's information system(s) or nonpublic information.

7. Cybersecurity Awareness Training Conducted at Least Annually for All Personnel and Updated to Reflect Risks Identified by the Most Recent Risk Assessment.

Employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat. Since identity theft is a leading cause of fraudulent distributions, it should be considered a key topic of training, which should focus on current trends to exploit unauthorized access to systems. Be on the lookout for individuals falsely posing as authorized plan officials, fiduciaries, participants or beneficiaries.

8. Secure System Development Life Cycle Program (SDLC).

A secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort. Best practices include:

- Procedures, guidelines, and standards which ensure any in-house applications are developed securely. This would include such protections as:
  - » Configuring system alerts to trigger when an individual's account information has been changed.
  - » Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account.
  - » Requiring additional validation for distributions (other than a rollover) of the entire balance of the participant's account.
- Procedures for evaluating or testing the security of externally developed applications including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests, particularly with respect to customer-facing applications.

9. A Business Resiliency Program which Effectively Addresses Business Continuity, Disaster Recover, and Incident Response.

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. The core components of a program include the Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan.

- The Business Continuity Plan is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption.
- The Disaster Recovery Plan is the documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption.
- The Incident Response Plan is a set of instructions to help IT staff detect, respond to, and recover from security incidents.

An effective Business Resiliency Program should:

- Reasonably define the internal processes for responding to a cybersecurity event or disaster.
- Reasonably define plan goals.
- Define the documentation and reporting requirements regarding cybersecurity events and responses.
- Clearly define and describe the roles, responsibilities, and authority levels.
- Describe external and internal communications and information sharing, including protocols to notify plan sponsor and affected user(s) if needed.
- Identify remediation plans for any identified weaknesses in information systems.
- Include after action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
- Be annually tested based on possible risk scenarios.

10. Encryption of Sensitive Data Stored and in Transit.

Data encryption can protect nonpublic information. A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.

11. Strong Technical Controls Implementing Best Security Practices.

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Best security practices for technical security include:

- Hardware, software and firmware models and versions that are kept up to date.
- Vendor-supported firewalls, intrusion detection and prevention appliances/tools.
- Current and regularly updated antivirus software.
- Routine patch management (preferably automated).
- Network segregation.
- System hardening.
- Routine data backup (preferably automated).

12. Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its participants, 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 complying with agreed upon notification requirements.
- Fixing the problems that caused the breach to prevent its recurrence.

LAW360®

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Cybersecurity Insights From ERISA Rulings, DOL Advice

By **Richard Nowak and Alexander Vitruk** (June 14, 2021, 2:03 PM EDT)



Richard Nowak



Alexander Vitruk

Cybersecurity has become critically important to plan sponsors, plan administrators and plan participants. With retirement plans holding an estimated $9.3 trillion in assets as well as sensitive information for approximately 140 million plan participants,[1] retirement accounts are especially attractive targets for cyber-enabled fraud.

For instance, sophisticated phishing email schemes have proliferated during the COVID-19 pandemic, threatening retirement accounts.[2] Ever-expanding technology connecting data and people has also opened the door to bad actors.[3]

This article explores the expanding intersection of the Employee Retirement Income Security Act[4] and cybersecurity issues, focusing on recent court decisions as well as guidance from the U.S. Department of Labor.

ERISA Claims Based on Cybersecurity Issues

As more and more cyber breaches pervade the industry, plan sponsors and administrators should be cognizant of fiduciary risk.

As litigation has already shown, a new argument in ERISA cases is that ERISA's duty of prudence — which obligates fiduciaries to act with the care, skill, prudence and diligence of a prudent man when satisfying their obligations to the plan — requires fiduciaries to take appropriate steps to safeguard sensitive participant data and participants' benefits.[5] While these are relevantly new issues, courts around the country have started shaping the intersection of ERISA and cybersecurity.

In Leventhal v. MandMarblestone Group LLC,[6] for instance, the U.S. District Court for the Eastern District of Pennsylvania in May 2019 concluded that the plaintiff had pled a plausible fiduciary breach related to cybersecurity incidents.

In Leventhal, a participant in the Leventhal Sutton & Gornstein 401(k) profit-sharing plan allegedly withdrew money from his plan account by emailing a withdrawal request form that was intercepted by unknown criminals who posed electronically as his office administrator and sent fraudulent withdrawal forms to the defendants — the alleged plan fiduciaries.[7] The fraudulent withdrawal forms purportedly requested that the defendants send the participant's account funds to a bank account that did not belong to the plaintiff and had never been used by him.

The district court found that the plaintiffs had plausibly stated an ERISA breach of fiduciary duty claim because they alleged that they had obtained documents from the defendants showing that the defendants were aware of the peculiar nature and frequency of the fraudulent withdrawal forms, but failed to alert the plaintiffs or verify the requests.[8] The district court also credited the plaintiffs' allegations that the defendants had failed to implement the typical procedures and safeguards used to notify participants of strange requests and/or verify the requests.[9]

An April 2021 decision from the U.S. Court of Appeals for the Ninth Circuit, Pruchnicki v. Envision Healthcare Corp.,[10] may also have broader implications for ERISA matters stemming from cybersecurity issues. Although she did not allege any claims under ERISA, the plaintiff alleged four categories of injury stemming from a data breach[11] of the defendants' systems:

- Lost time spent reviewing consumer credit reports, obtaining new credit cards, checking financial accounts, and answering an increased number of spam calls;
- Emotional distress, including stress, nuisance and annoyance from dealing with the effects of the breach; worry, anxiety and hesitation when applying for new credit cards; and concern that damage to her creditworthiness could affect her ability to obtain credit for her business;
- Imminent and certainly impending injury flowing from potential fraud and identity theft; and
- Diminution in value of her personal and financial information.[12]

The Ninth Circuit affirmed the district court's dismissal of the case on the ground that, although the plaintiff alleged sufficient injury in fact to support standing,[13] she had failed to establish compensable damages, or out-of-pocket expenses. The Ninth Circuit explained that the plaintiff cited no authority recognizing lost time as a cognizable injury, failed to assert the existence of any physical injury or illness, and failed to allege that her personal information actually lost value.

This decision may be instructive for ERISA matters, at least within the Ninth Circuit, given that, to state an ERISA fiduciary breach claim, a plaintiff must establish harm.[14] The types of harm identified in Pruchnicki — e.g., lost time, emotional distress, diminution of value of personal information — may not be sufficient to sustain a fiduciary breach claim.

There are also a growing number of cases at the intersection of ERISA and cybersecurity. For example, participants have asserted ERISA claims in circumstances involving alleged identity theft and unauthorized distributions from their retirement accounts.[15]

Plan service providers and fiduciaries to retirement plans should be cognizant of not only ERISA's fiduciary requirements and the growing body of litigation involving participants who have suffered retirement plan losses due to cyberattacks, but also applicable state laws that provide for disclosure of personal or private information, such as North Carolina and California. Indeed, state attorneys general have been active in enforcing these laws in cyber breach matters.[16]

Given the DOL's current focus on cybersecurity issues, discussed below, and the likelihood that cybersecurity attacks on retirement accounts will persist and become more sophisticated, we expect to see an increase in the number of ERISA cases in this area.

Recent Guidance From the DOL

On April 14, the DOL **published written guidance** on cybersecurity issues concerning plan sponsors, plan fiduciaries, record-keepers and plan participants. Acknowledging that ERISA requires plan fiduciaries to take appropriate precautions to mitigate the risks of internal and external cybersecurity threats to participants and assets, the DOL issued its guidance in three parts:

- Tips for hiring a service provider with strong cybersecurity practices;
- Cybersecurity program best practices; and
- Online security tips.[17]

Hiring a Service Provider With Strong Cybersecurity Practices

The DOL guidance offers various suggestions for hiring and monitoring a service provider to help plan fiduciaries meet their responsibilities under ERISA. Those tips included:

- Compare the service provider's information security standards, practices and policies, audit results to standards adopted by other financial institutions, and seek providers that engage a third-party auditor to review and validate its program.
- Seek contract provisions that give the right to review audit results.
- Evaluate the provider's track record in the industry with respect to security incidents, litigation and legal proceedings.
- Inquire about past security breaches and how the provider responded.
- Find out if the provider's insurance policies would cover losses covered by cybersecurity and identity theft breaches.
- Ensure that the contract requires ongoing compliance with cybersecurity and information security standards; avoid contract provisions that limit the service provider's responsibility; and include contract provisions that would enhance cybersecurity protection for the plan and its participants.[18]

Although the DOL's cybersecurity suggestions are memorialized in subregulatory guidance, as opposed to a formal regulation, plan sponsors and fiduciaries should keep this guidance in mind when hiring and retaining plan service providers.

Accordingly, plan sponsors and fiduciaries should consider reviewing their current hiring practices and service provider contracts to see whether they meet the suggested standards. Among other things, plan sponsors and fiduciaries should carefully review any contractual language limiting the service provider's liability and obligations in the event of a breach.

And, consistent with their existing monitoring efforts, plan sponsors and fiduciaries should consider engaging in periodic third-party audits and reviews of the service provider's track record — e.g., security incidents, litigation, etc. Indeed, cybersecurity practices should be a focus of any request for proposal and part of any ongoing reviews of service providers — e.g., requests for proposals should seek information about data security and data transmittal policies, insurance coverage, etc.

Future plaintiffs may rely on the DOL's recent guidance in arguing that there is a duty to safeguard plan assets against unauthorized withdrawals and that plan fiduciaries also have a duty to take sufficient steps to properly select and monitor a service provider's cybersecurity policies.

On the flip side, plan fiduciaries who undertake those steps may have a stronger defense against such actions. Moreover, those steps should be accurately and thoroughly reflected in fiduciary committee minutes and materials to document a prudent process and thereby minimize risk of fiduciary liability.

Cybersecurity Program Best Practices

With respect to cybersecurity program best practices, the DOL provides recommendations to service providers to assist them in developing and maintaining an effective cybersecurity program.

Though these best practices are directed toward service providers, the DOL also emphasizes that: "Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks," which includes making "prudent decisions on the service providers they should hire."

The DOL's recommendations include, among other things:

- Have a formal, well-documented cybersecurity program that is reviewed annually, approved by senior leadership, explained effectively to users, and reviewed by an independent auditor.
- Conduct and document prudent annual risk assessments.
- Have strong access control procedures, including with respect to authentication and authorization.
- Ensure 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.
- Conduct periodic cybersecurity awareness training, at least annually for all personnel and update it to reflect risks identified by the most recent risk assessment.
- Implement strong technical controls in accordance with best security practices, including routine data backup and patch management, up-to-date hardware, software, firmware and antivirus software, and network segregation.[19]

Plan service providers should consider incorporating language into their service contracts on compliance with these recommended best practices going forward. Moreover, as discussed above, the recent ERISA matters based on cyberattacks have generally involved cyber criminals posing as participants, often calling into the record-keeper's service center to obtain participant data.

As such, having an effective customer call center authentication process is important.[20] Customer service representatives should be trained to ask callers to verify items such as their date of birth, home address and other personal identifying information. A more sophisticated customer call center authentication process may involve tokens associated with a caller's phone or carrier, or a multifactor authentication system that can understand the characteristics of certain sounds that can be translated into a voice print.[21]

Plan fiduciaries should monitor whether service providers have such practices in place. This is especially important in the wake of any breach. Indeed, cybersecurity breaches often involve service providers who handle day-to-day administration for retirement plans.

For example, NOW: Pensions, a UK pensions provider, was the victim of a data breach by an unknown third party during a three-day period in December 2020. It resulted in the personal information of 30,000 customers being posted on the internet, and the company blamed the data breach on one of its service providers.[22]

When faced with such a breach, an organization may be inclined to terminate its service provider. In some cases, there may be grounds to terminate the relationship — e.g., the provider may have failed to comply with the parties' contract or applicable law. But there may also be compelling reasons to retain the provider — e.g., there is a dependable relationship and the provider's unique products or services are critical to the organization.

Plan sponsors and administrators should consider different factors in making such a consequential decision to determine whether it is in the best interest of the plan and its participants. They should also carefully evaluate and document — and revise as appropriate — their measures and processes in the wake of any breach.

Online Security Tips

Finally, the DOL offered online security tips to plan participants to help reduce their own risk of retirement account fraud and loss. Those tips include:

- Register, set up and routinely monitor online accounts.
- Use strong and unique passwords.
- Use multifactor authentication;
- Keep personal contact information current.
- Close or delete unused accounts.
- Be wary of free Wi-Fi.
- Beware of phishing attacks.
- Use anti-virus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents.[23]

Although the DOL's online security tips are primarily directed toward participants, plan sponsors and fiduciaries should consider providing and documenting education on cybersecurity issues to their participants.

For instance, they could provide clear guidance in the summary plan description, regularly issue best practices notices to participants, and organize educational seminars.

Not only is cybersecurity education important to help participants protect their own financial well-being, taking active steps to help participants understand potential cybersecurity and data privacy risks may reduce the risk of litigation against the plan sponsor and the plan's fiduciaries and help them defend against future claims.

Conclusion

Cybersecurity has become an area of critical importance to plan sponsors, plan administrators and plan participants.

Plan sponsors and administrators are well advised to follow the growing body of litigation involving participants who have suffered retirement plan losses due to cyberattacks, and to evaluate their cybersecurity programs, protocols and contracts against the DOL's recent three-part guidance.

Richard E. Nowak is a partner and Alexander Vitruk is an associate at Mayer Brown LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] U.S. Dep't of Labor, News Release, US Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, Plan Participants (April 14, 2021), available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414.

[2] See Alessandra Malito, Hackers Are Ramping Up Attacks on Retirement Accounts – How to Keep Yourself Safe, MarketWatch, (Feb. 6, 2020), available at https://www.marketwatch.com /story/how-to-keep-your-retirement-accounts-safe-2020-01-28.

[3] See Rebecca Moore, Expansion of Technology Will Increase Cyber Security Threats, Plan Sponsor, (Feb. 15, 2019), available at https://www.plansponsor.com/expansion-technology-will-increase-cyber-security-threats/.

[4] 29 U.S.C. § 1001 et seq.

[5] See ERISA § 404(a)(1)(B), 29 U.S.C. § 1104(a)(1)(B).

[6] Leventhal v. MandMarblestone Grp. LLC , No. 18-CV-2727, 2019 WL 1953247 (E.D. Pa. May 2, 2019).

[7] 2019 WL 1953247 at *2. The named plaintiffs were participant Jess Leventhal, Leventhal

Sutton & Gornstein 401(k) Profit Sharing Plan, and Leventhal Sutton & Gornstein, Attorneys at Law.

[8] Id. at *6.

[9] Id.

[10] Pruchnicki v. Envision Healthcare Corp ., 845 F. App'x 613 (9th Cir. April 21, 2021).

[11] Plaintiff had provided her personal and/or financial information to defendants, according to the underlying complaint. See Pruchnicki v. Envision Healthcare Corp., 439 F. Supp. 3d 1226, 1229 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021).

[12] Pruchnicki, 845 F. App'x 613.

[13] The district court held, and the defendants conceded, that the plaintiff had standing based on allegations of future harm. Pruchnicki v. Envision Healthcare Corp., 439 F. Supp. 3d 1226, 1231 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021).

[14] See, e.g., Allen v. GreatBanc Tr. Co ., 835 F.3d 670, 678 (7th Cir. 2016); see also Wise v. MAXIMUS Fed. Servs., Inc ., 445 F. Supp. 3d 170, 196 (N.D. Cal. 2020) (same).

[15] See, e.g., Bartnett v. Alight Solutions, LLC, et al. , No. 20-CV-02127, 2021 WL 428820 (N.D. Ill. Feb. 8, 2021); Berman v. Alight Solutions, LLC, et al., No. 4:19-cv-06489-JST (N.D. Cal., filed Oct. 9, 2019).

[16] See, e.g., Press Release, Arizona Attorney General, Attorney General Mark Brnovich Files Lawsuit Against Google Over Deceptive and Unfair Location Tracking, (May 27, 2020), available at https://www.azag.gov/press-release/attorney-general-mark-brnovich-files-lawsuit-against-google-over-deceptive-and-unfair.

[17] U.S. Dep't of Labor, News Release, US Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, Plan Participants (April 14, 2021), available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414.

[18] U.S. Dep't of Labor, Tips for Hiring a Service Provider with Strong Cybersecurity Practices (April 14, 2021), available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf.

[19] U.S. Dep't of Labor, Cybersecurity Program Best Practices (April 14, 2021), available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

[20] Forrester Research, Best Practices: Customer Call Center Authentication, (March 22, 2019), available at https://www.forrester.com/report/Best+Practices+Customer+Call+Center+Authentication/-/E-RES141457.

[21] See Ben Rizzuto, Janus Henderson Investors, Protecting Plan Participants from Cyberthreats in the Age of Remote Working, (Oct. 28, 2020), available at https://www.janushenderson.com/en-us/advisor/article/protecting-plan-participants-from-cyberthreats-in-the-age-of-remote-working/.

[22] See Miles Brignall, Data Breach Hits 30,000 Singed Up to Workplace Pensions Provider, The Guardian, (Dec. 23, 2020), available at https://www.theguardian.com/technology/2020/dec/23/data-breach-hits-30000-signed-up-to-workplace-pensions-provider.

[23] U.S. Dep't of Labor, Online Security Tips (April 14, 2021), available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.

All Content © 2003-2022, Portfolio Media, Inc.