Cybersecurity Risk Assessment and Employee Benefit Plans: Fiduciaries' Duty to Protect Plan Information

THURSDAY, AUGUST 15, 2019, 1:00-2:50 pm Eastern

IMPORTANT INFORMATION FOR THE LIVE PROGRAM

This program is approved for 2 CPE credit hours. To earn credit you must:

- Participate in the program on your own computer connection (no sharing) - if you need to register additional people, please call customer service at 1-800-926-7926 ext. 1 (or 404-881-1141 ext. 1). Strafford accepts American Express, Visa, MasterCard, Discover.
- **Listen on-line** via your computer speakers.
- **Respond to five prompts during the program plus a single verification code.**
- To earn full credit, you must remain connected for the entire program.

WHO TO CONTACT DURING THE LIVE PROGRAM

For Additional Registrations:
-Call Strafford Customer Service 1-800-926-7926 x1 (or 404-881-1141 x1)

For Assistance During the Live Program:
-On the web, use the chat box at the bottom left of the screen

If you get disconnected during the program, you can simply log in using your original instructions and PIN.

Tips for Optimal Quality

FOR LIVE PROGRAM ONLY

Sound Quality

When listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, please e-mail sound@straffordpub.com immediately so we can address the problem.

Cybersecurity Risk Assessment and Employee Benefit Plans: Fiduciaries' Duty to Protect Plan Information

August 15, 2019

Amy M. Gordon, Partner
Winston & Strawn
amgordon@winston.com

Allison Itami, Principal
Groom Law
aitami@groom.com

Jesse St.Cyr, Partner
Poyner Spruill
jcyr@poynerspruill.com

Notice

ANY TAX ADVICE IN THIS COMMUNICATION IS NOT INTENDED OR WRITTEN BY THE SPEAKERS' FIRMS TO BE USED, AND CANNOT BE USED, BY A CLIENT OR ANY OTHER PERSON OR ENTITY FOR THE PURPOSE OF (i) AVOIDING PENALTIES THAT MAY BE IMPOSED ON ANY TAXPAYER OR (ii) PROMOTING, MARKETING OR RECOMMENDING TO ANOTHER PARTY ANY MATTERS ADDRESSED HEREIN.

You (and your employees, representatives, or agents) may disclose to any and all persons, without limitation, the tax treatment or tax structure, or both, of any transaction described in the associated materials we provide to you, including, but not limited to, any tax opinions, memoranda, or other tax analyses contained in those materials.

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your tax adviser.

Cybersecurity Risk Assessment and Employee Benefit Plans: Fiduciaries' Duty to Protect Plan Information

Amy Gordon
Amgordon@Winston.com
312-558-6390

Allison Itami
aitami@groom.com
202-861-0159

Jesse St.Cyr
jcyr@poynerspruill.com
919-783-2880

WINSTON & STRAWN LLP

GROOM LAW GROUP

Poyner Spruill LLP

Why Focus on Cybersecurity

- Data breach prevention and response is an increasingly pressing issue for many industries, including employee benefit plans
- Employee benefit plans face significant cybersecurity threats
- Given the incredibly significant amount of assets involved, the consequences of even one single attack can be devastating
- There are numerous interfaces that provide potential entryways for cybercriminals
- A diligent plan fiduciary will take steps to prevent a cyber-breach

Cybersecurity Open Questions

- Is cybersecurity an ERISA fiduciary responsibility?
  - If not, should it be?
  - If so, does ERISA preempt state cybersecurity laws?
    - It is not clear that state privacy or cybersecurity statutes would be preempted by ERISA
- Plan sponsors and service providers already take seriously their responsibilities to protect participant data, but where are the lines of responsibilities and accountability in the event of a breach?

Health Plans vs. Retirement Plans

- Health Plans are subject to the Health Insurance Portability and Accountability Act as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH") (herein "HIPAA")
- Health Plans and Retirement Plans are also subject to state privacy laws
  - Some states have started to create their own laws which typically address breach notifications and private rights of action for any unauthorized disclosures of protected personal information
  - HIPAA set a floor not a ceiling on regulation
  - Several state attorneys general have been active in enforcing these laws in cyberbreach cases, but a state-by-state framework remains inconsistent in that regard

Retirement Plans

- There is no comprehensive federal regulatory scheme governing cybersecurity for retirement plans in the US
- ERISA is silent on data protection in the form of electronic records
- US courts have not yet decided whether managing cybersecurity risk is a fiduciary function
- There is no comprehensive federal scheme that covers all service providers, (not all service providers are subject to GLBA)
- Many service providers that service the retirement market are covered by federal rules based on their industry
  - However, note that these plan service providers often cross several different industries, making standard compliance rules difficult

Heath Plans and HIPAA Breaches

- A HIPAA Breach means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) which compromises the security or privacy of such information
- PHI Means:
  - Information that relates to the past, present, or future
    - Physical or mental health condition;
    - Payment for health care; or
    - Provision of health care; and
  - Identifies or can be used to identify the individual, e.g., name, address, employer, date of birth, e-mail address, telephone and fax, social security number, photos, vehicle number, license number, date of death, etc.; and
  - Relates to the HIPAA covered entity

Non-HIPAA Breach

- A breach does not include:
  - Unintentional acquisition, access, or use by an employee or individual acting under the authority of the covered entity or a business associate if done in good faith and within the scope of employment or other professional relationship with the covered entity or business associate and such information is not further improperly acquired, accessed, used, or disclosed by any person, or
  - Any inadvertent disclosure from a covered entity to another covered entity, or
  - A disclosure to a person who would not reasonably have been able to retain the information

Safeguarding PHI is Critical

- If unsecured PHI is accessed, the covered entity must notify affected individuals
- Unsecured PHI means PHI that is not secured through the use of technology or methodology specified by the Secretary of HHS in issued guidance
  - For Electronic PHI (EPHI), this requires encryption following specific HHS standards

Presumption that a Breach has Occurred

- Any unauthorized acquisition, access, use or disclosure of PHI is presumed to be a breach
- Notification of a breach is required unless the covered entity or business associate demonstrates through a risk assessment there is a low probability that the PHI has been compromised - the burden is on the covered entity or business associate to rebut the presumption

Breach Risk Assessment

- The risk assessment must consider:
  - The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification
  - The unauthorized person who use the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to PHI has been mitigated

A HIPAA breach may also be a violation of state law – state breach notification laws often have different breach definitions and requirements

Breach Notification Requirements

- Notification to affected individuals must be made without unreasonable delay no later than 60 days after discovery of the breach by the covered entity (60 days is an outer limit)
- Discovery of a breach by any someone employed by the covered entity, is notice to the covered entity
- If there is a breach by a business associate, the business associate must provide notice to the covered entity without unreasonable delay no later than 60 days after discovery; the covered entity then has up to 60 days to notify affected individuals
- If a business associate is the covered entity's "agent", then discovery of a breach by the business associate is also attributed to the covered entity
- If some individuals cannot be notified, posting on the covered entity's benefits website and/or in print or broadcast media may be required

Enforcement of HIPAA Rules

- HHS must perform periodic audits of covered entities and business associates (previously, HHS investigations were complaint-based)
- Mandatory HHS investigation of any complaint if a preliminary investigation of the complaint indicates a possible violation due to willful neglect
- HHS has discretion to proceed directly to formal enforcement action to impose penalties for violations
- State attorneys general may now bring a civil action on behalf of residents of the State to enjoin further violation - States can obtain damages up to $100 per violation, not to exceed $25,000 for a year

Liability Under HIPAA

- Civil penalties - can now be $50,000 or more for each violation, up to a maximum of $1,500,000 for violations of the same requirement; penalty amount depends on circumstances - penalties are mandatory for willful neglect
- Criminal penalties - $50,000 and/or one year in prison for wrongful disclosure, and up to $250,000 and/or ten years in prison for offenses committed with the intent to sell information
- Disciplinary action by the covered entity, including termination of employment (depending on severity)

Numerous Interfaces Increase Risk

- Retirement plans, 401k plans, and 403b plans are typically administered by numerous parties. In addition to the plan sponsor, there is typically a trustee, and a plan administrator (record keeper)
- Health and welfare plans have insurers or third party administrators, a custodian or trustee (sometimes) and the plan sponsor
- Participants can log into benefit portals through their home, phone and/or work computers

Government Efforts Regarding Cybersecurity

- United States Department of Labor's (Department) Advisory Group
  - The duties of the Council are to advise the Secretary of the United States Department of Labor (Secretary) and submit recommendations regarding the Secretary's functions under ERISA
  - In November of 2016, the Council provided the Secretary a report titled, Cybersecurity Considerations for Benefit Plans
  - The Council 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
  - The Counsel recommended that plan sponsors and providers should approach cyber-risk management strategies with the understanding that a good program will not eliminate risks, but rather manage them

Government Efforts Regarding Cybersecurity

- United States Department of Labor's Advisory Group
  - The ERISA Advisory Council is asking the DOL to provide guidance on how to evaluate the cybersecurity risks they face and to require retirement plan sponsors to be familiar with the various security frameworks used to protect data as well as to build a cybersecurity process
  - The Council would also like the DOL to recommend that sponsors use third-party risk management
  - While ERISA does not mandate a written cybersecurity policy, plan sponsors are required to always act prudently and to document that process, and cybersecurity should be part of that process, according to the white paper [https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2018/12/WP-2018-16-Rouse-et-al.pdf]

ERISA Fiduciary Rules in General

- ERISA fiduciary standards are described as "the highest known in law"
- Must act solely in the interest of participants and beneficiaries, for the exclusive purpose of:
  - providing benefits; and
  - defraying reasonable administrative costs
- Must act:
  - with the care, skill, prudence, and diligence;
  - that a prudent person;
  - acting in a like capacity and familiar with such matters;
  - would use in similar circumstances

Fiduciary Delegation

- If fiduciary lacks expertise, must hire appropriate experts
- Fiduciaries may delegate certain duties, but the fiduciary remains responsible for monitoring delegates

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- To educate and assist plan sponsors in their compliance efforts, the Council created the Cybersecurity Considerations Document
  - Prevention of a cybersecurity threat is impossible, but there are steps that can be taken to limit the threat
  - At present, there is no consensus within the industry regarding which cybersecurity framework constitutes a 'best practice' approach
  - Not a "one-size-fits-all" approach
  - Determine what is reasonable from a commercial perspective and an ERISA perspective for each plan
  - The cybersecurity risk management strategy cannot be a static checklist
  - The program should include regular reporting, frequent reviews and process updates that are specifically tailored to the plans' needs

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take
  - Inventory the plan's data, and consider using, sharing and maintaining only the minimum amount of data necessary. This applies to the plan sponsor's data, as well as that used, shared and maintained by service providers
  - Devise a framework upon which to base a cybersecurity risk management strategy (e.g., the NIST framework or the SAFETY Act as models or possible starting points)
  - Establish a process that includes, implementation, monitoring, testing and updating, reporting, training, controlling access, data retention and/or destruction, and third party risk management

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take
  - Balance the scope and cost of a cyber-risk management strategy against the size and sophistication of the plans and the plan sponsor
  - Decide what if any portion of the cyber-risk management costs should be borne by the plan, versus the plan sponsor, including insurance
  - Ensure that any program also addresses any state specific cyber-risk requirements

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take Relating to Service Providers
  - Review applicable contract provisions with service providers, and require vendors to attest that the service provider or vendor has proper procedures in place to protect the plan's data
  - Plan sponsors should monitor the cyber protocols and practices of these providers on an on-going basis to ensure they are robust enough
  - Plan sponsors, fiduciaries and third party service providers may want to consider whether SAFETY Act certifications could fit into their overall cybersecurity risk management strategy
    - Plan sponsors can take advantage of the Act's liability protections by retaining vendors that have or use SAFETY Act approved processes or procedures

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take Relating to Insurance
  - Plan sponsors should evaluate their insurance coverage/bonding policies to ensure they are covered in the case of a cybersecurity attack
  - A Fiduciary may look into purchasing an insurance policy or bond to protect against potential loss to the plan and plan participants
  - Discussions with insurance brokers has led us to understand that a few different coverages (e.g., a cyber-policy, a crime policy, errors and omissions and fiduciary insurance) may all need to be bundled to provide a comprehensive solution
  - It is also important to address cyber-breaches which can occur at different plan interfaces, e.g. at the trustee, participant or administrator's interface

Prudent Steps ERISA Plan Fiduciaries Should take to Address Cybersecurity

- Steps to Take Relating to Insurance
  - It is also important to address cyber-breaches which can occur at different plan interfaces, e.g. at the trustee, participant or administrator's interface
    - A negative factor with respect to insurance coverage is where the actual cyber-breach occurs may dictate whether the insurer will pay the claim
    - Unless the cyber-breach occurs at the plan sponsor's interface, the claim may be refuted
    - Even if a plan sponsor has adequate insurance coverage, the insurer may refuse to pay a claim if the breach happens at the site of the service provider, or if the plan participant's negligence led to the breach
    - It is critical to get counseling on the appropriate Cyber Insurance plan to cover your specific needs

Government Efforts Regarding Cybersecurity

- HELP Committee GAO Request 2019
- EBSA Audit Requests
- Congress enacted the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (SAFETY Act)
  - Encourages the use of anti-terrorism products, services and technologies in civilian settings
  - The SAFETY Act specifically provides risk management protections to firms that develop, sell or deploy these technologies, as well as contractors, subcontractors and consumers downstream
  - The SAFETY Act protections include liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where Qualified Anti-Terrorism Technologies (QATTs) have been deployed

Private and Not-For-Profit Cybersecurity Organizations

- Not unique to employee benefit plans, significant cybersecurity efforts have been, and continue to be, developed to help organizations manage and navigate cyber-risk
- Health Information Trust Alliance (HITRUST)
  - A privately held company
  - Established a Common Security Framework (CSF), tools and cyber-risk Management Framework (RMF) that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data
  - The CSF includes a prescriptive set of controls that seek to harmonize the requirements of multiple regulations and standards

Private and Not-For-Profit Cybersecurity Organizations

- The American Institute of Certified Public Accountants (AICPA)
  - They prepared a Q&A by the EBPAQC to help plan auditors understand cybersecurity risk in employee benefit plans, and to discuss cybersecurity risk, responsibilities, preparedness, and response with plan clients
  - https://www.aicpa.org/content/dam/aicpa/interestareas/employeebenefitplanauditquality/resources/accountingandauditingresourcecenters/downloadabledocuments/cybersecurity-and-ebp-questions-and-answers.pdf

Private and Not-For-Profit Cybersecurity Organizations

- The SPARK Institute
  - A private sector initiative that is working on establishing uniform data management standards for the defined contribution retirement plan market
  - SPARK has established a Data Security Oversight Board (DSOB) that oversees program development and implementation
  - The DSOB includes representatives from plan administrators, consultants, SPARK staff and Department of Homeland Security
  - Issued a best practices report on September 20, 2017
  - http://www.sparkinstitute.org/pdf/SPARK%20Data%20Security%20Industry%20Best%20Practice%20Standards%209-2017.pdf

Other Helpful Resources

- AICPA (2017). AT-C Section 215: Agreed-Upon Procedures Engagements. Association of International Certified Professional Accountants. https://www.aicpa.org/research/standards/auditattest/downloadabledocuments/at-c00215.pdf
- ERISA Advisory Council (ERISA) (2016). Cybersecurity Considerations for Benefit Plans. Report to the Honorable Thomas E. Perez, United States Secretary of Labor. https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisorycouncil/2016-cybersecurity-considerations-for-benefit-plans.pdf
- Federal Trade Commission (2002). How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act. Washington, DC: FTC. https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacyconsumer-financial-information-rule-gramm-leach-bliley-act.pdf
- The SPARK Institute (2017). 'Industry Best Practice Data Security Reporting.' SPARK Institute Release 1.0. September 20. http://www.sparkinstitute.org/pdf/SPARK%20Data%20Security%20Industry%20Best%2 0Practice%20Standards%209-2017.pdf
- Tech World (2017). 'The Most Infamous Data Breaches.' Tech World. December 6: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/
- US Department of Labor (2017). Guidance on the Protection of Personal Identifiable Information. https://www.dol.gov/general/ppii