What is Your Mother's Maiden Name?
Privacy and Security Considerations for Employee Benefit Plans

September 24, 2020

Presented by:
Joe Adams, Partner
Amy Gordon, Partner
Alessandra Swanson, Partner
Eric Shinabarger, Associate

WINSTON & STRAWN LLP

Focusing on Cybersecurity

- Employee benefit plans face significant cybersecurity threats
- A diligent plan fiduciary will take steps to prevent a successful cyber attack

Why Are Benefit Plans Targeted?

- Given the incredibly significant amount of personal information and the financial assets an employee benefit plan possesses, the consequences of even one single attack can be devastating
- There are numerous interfaces that provide potential entryways for cybercriminals

Numerous Interfaces

- Retirement plans, 401(k) plans, and 403(b) 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
- Plan sponsors have no control over these interfaces

Working From Home

- Given the current COVID-19 landscape, many people are working from home, so they are logging in through personal computers, company-provided laptops, and through unsecured internet
- Even without COVID-19, participants can log into benefit portals through their home, phone, and/or work computers

Cybercriminals are Upping Their Game

- Cybercriminals are working harder to exploit the vulnerabilities of COVID-19
- Headlines are constantly mentioning companies and individuals who are being hacked
- These are the type of accounts that individuals do not often check, so it may be easier to initiate a transaction without detection
- Cybercriminals can leverage credentials that are re-used by individuals for other accounts that have been breached

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
- Industry leaders seek guidance from the IRS and Treasury
- 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?

Current Government Landscape

- There is no comprehensive federal regulatory scheme governing cybersecurity for retirement plans in the U.S.
- ERISA is silent on data protection in the form of electronic records
- U.S. courts are evaluating 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 the Gramm–Leach–Bliley Act)

Current Government Landscape

- 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
- 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
- Several state attorneys general have been active in enforcing these laws in cyber breach cases, but a state-by-state framework remains inconsistent in that regard

Government Efforts Regarding Cybersecurity

- United States Department of Labor's (Department) Advisory Group (the Council)
  - 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 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
  - 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]

Breach Causes of Action and Lawsuits

- Data breach laws historically have not included a private right of action with statutory damages
  - For example, the Health Insurance Portability and Accountability Act of 1996
- Recent trends towards private rights of action and statutory damages
  - For example, the California Consumer Privacy Act
- The Department has begun to investigate service providers with respect to ERISA and cybersecurity
- Employers are being sued based on a breach of fiduciary duty and/or state privacy causes of action
  - For example, when bad actors hack into a participant's 401(k) account and take a distribution

What Should a Fiduciary Do?

- Mitigate risk through
  - Education
  - Tightening procedures
  - Insurance
  - Contractual protections

Educate Participants and Employees

- Teach employees and participants what they can do to protect information
- Impose working-from-home protocols
- The Cybersecurity & Infrastructure Security Agency offers some good resources on cyber protection
- https://www.cisa.gov/publication/cyber-essentials-toolkits

Tightening Procedures

- Prevention of a cybersecurity threat is impossible, but there are steps that can be taken to limit the threat
  - 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
  - Establish a process that includes implementation, monitoring, testing and updating, reporting, training, controlling access, data retention and/or destruction, and third-party risk management
  - 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

Tightening Procedures

- For example, in all employee benefit plans
  - Work with vendors to strengthen security safeguards
  - Prohibit participants from reusing usernames/passwords or security questions
  - Notify employees that they need to comply with the security protocols of service provider if they want to ensure the protections from those service providers
- For example, in the 401(k) area
  - Increased security and password requirements (e.g., mandatory two-factor authentication and more stringent minimum password security standards)
  - Organizational measures, such as implementing red flag triggers and requiring disbursement confirmations
  - Prepare for an incident
    - Have procedures in place to flag questionable or illegal activity
    - Know how this will affect other accounts

Not a “one-size-fits-all” approach

- At present, there is no consensus within the industry regarding which cybersecurity framework constitutes a “best practice” 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

Insurance

- Plan sponsors should evaluate their insurance coverage/bonding policies to ensure they are covered in the case of a cybersecurity attack
- 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

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
- Require insurance protections in service provider agreements

Contractual Protections

- Ownership of the information
- Breach reporting and investigation obligations
- Subcontractor issues
- Specific data security provisions and auditing rights
- Shipping information off-shore
- Indemnification and limitations of liability

These are all items to consider including in, and discussing during, the RFP process