Wagner Law Group and Segal

Cybersecurity

Keeping Retirement Benefit Plans and Plan Administration Secure

Stephen Wilkes and Susan Rees, Wagner Law Group / **Diane McNally**, Segal

October 2020

THE WAGNER LAW GROUP

Segal

Today's Presenters

Stephen Wilkes
Wagner Law Group

Susan Rees
Wagner Law Group

Diane McNally
Segal

Agenda

Introduction — Why Protecting Plan Data and Assets Matters?

ERISA — The Law, DOL Guidance, Recent Cases

Best Practices for Plan Administrators

Cyber Insurance and Breach Response

Summary

Introduction

- Retirement plans use electronic means for disclosures to participants and to conduct participant transactions such as distribution requests.
- What do we mean by “cybersecurity”?
  - Measures taken by plan fiduciaries to protect against unauthorized electronic withdrawals from participant accounts and electronic misappropriation of participant personal information (PPI).
  - PPI is any identifying data – birth date, social security number, account number, name of bank, email address, passwords.
- ERISA generally requires plan administrators as fiduciaries to protect the confidentiality of PII and the safety of plan accounts, but there are no specific fiduciary standards or guidance from the Department of Labor.
- DOL has provided limited guidance on electronic furnishing of required ERISA disclosures, requiring plan administrators to take measures “reasonably calculated” to protect the confidentiality of PPI.
- There are increasing occurrences of cybersecurity breaches involving plan data or plan assets. Thus, cybersecurity has broader application than to furnishing ERISA disclosures.
- Discussion of the law, current cases and best practices.

ERISA, the Law, DOL Guidance and Recent Cases

ERISA – The Law

- ERISA requirements will predominate because ERISA preempts most state laws, but in the cybersecurity cases, state laws may well apply.
- ERISA SECTION 404 – ". . .a fiduciary shall discharge his duties . . .with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims . . ."
- Every plan fiduciary with responsibility or discretion to create or administer plan cybersecurity measures is held to the standard of an expert in the field – the standard is the industry standard then prevailing.
- Compliance focusses on process. To be in compliance with the "prudent expert" standard, plan administrators need to stay up to date with current and ever-changing industry wide cybersecurity practices, including training and retraining personnel to avoid human error.
- Plan administrators are responsible for selecting and monitoring all plan service providers who have access to PII to ensure that the service provider uses and follows the cybersecurity procedures the plan administrator has adopted for itself. The service contracts should be explicit about responsibility.
- TPAs must also diligently monitor themselves for effective cybersecurity protections. TPAs that are not formally recognized as plan fiduciaries may be deemed to be "functional fiduciaries" if the TPA is responsible for a cybersecurity breach.

Pending and Recent Cybersecurity Fiduciary Breach Cases

Human error results in loss of assets from participant's account

- *Barnett v. Abbott Laboratories, Alight Solutions, et al.,* No. 2020 CV 2127, (N.D. Ill. filed April 3, 2020). Currently, the plan has been provisionally dismissed from the case, but the TPA found to be potentially liable under ERISA as a "functional fiduciary" and under state consumer protection law. The thief used participant information commonly found on the internet and then tricked a TPA employee into making distribution to a bank account set up by the thief. There are allegations that the cybersecurity precautions are inadequate, as are the procedures for notice to the participant which would have alerted her to the pending misappropriation. Important to note in this case that the DOL is investigating. *Scalia v. Alight Solutions,* LLC, 1:20-cv-02138 (N.D. Ill. April 6, 2020).

- *Leventhal v. MandMarblestone Group.* LLC, No. 18-cv-2727 (E.D. Pa. May. 27, 2020). In a preliminary motion, court ruled that the plan administrator and the TPA are jointly and severally liable if a fiduciary breach is proven. In this case a thief obtained a copy of the participant's distribution form, perhaps from the participant's private email account, which the employer allowed her to use for her employment. Thief then redirected distributions to its own accounts. There are also allegations that the cybersecurity precautions at the point of distribution were inadequate.

- *Berman v. Estee Lauder Inc., Alight Solutions, et al.,* No. 3:19-cv-06489, (N.D. Cal. filed October 9, 2019, settled in March 2020). Similar to the Abbott case, involves the same TPA (Alight), and apparently, the DOL also investigated.

Data breach multistate class actions

In re Anthem – PII held by Health Care system and numerous subsidiary entities was hacked. Class action under ERISA and state law settled in 2020, after lengthy litigation including one 70-page preliminary decision on which state laws may be used in addition to the ERISA claims.

DOL Guidance

Recent DOL guidance provides a safe harbor which permits plan administrators to use certain electronic media to furnish ERISA-required “covered” disclosures to certain “covered” participants and beneficiaries. The safe harbor offers three options:

1. Furnish to covered participant’s private email account or smart phone number if voluntarily provided, or if required by employer to be provided as a condition of employment.

2. Furnish to an employer-provided email account, but only if the email account is regularly used for other employer-related purposes.

3. Furnish on a website proceeded by notices of internet availability (NOIAs) on when and how to access, sent to the email accounts provided under # 1 or # 2.

Under any option, the plan administrator and any TPA must take measures “reasonably calculated” to protect the confidentiality of PII. Note that the safe harbor will not apply to participants for whom the electronic email alternatives are unavailable.

DOL Guidance

The DOL preamble states that the 404 duty of prudence requires that plan administrators monitor service providers who have access to PII, and states that the "covered" disclosures are also protected by the 404 duty to protect confidentiality.

There is uncertainty in light of current litigation, and the mixed message from the DOL. To the extent that required disclosures contain PII, the prudent plan administrator might want to consider:

- What protective steps are prudent if plan uses the participant's private email?
- Should the employer be willing to use its email system for the ERISA disclosures? The plan may be protected from state privacy laws by ERISA preemption, but the employer might be held responsible under state law for the consequences of any hacking?
- Notice the tension between protecting confidentiality and actual delivery of the documents. Will the website posting method, with its two step process result in effective disclosures, (i.e., "actual knowledge" of the information in disclosure) to participants and beneficiaries as required for statute of limitations purposes in the recent Supreme Court decision in *Sulmya v. Intel?* Should the plan consider track and verify methods?

Other Laws

- There may be interpretive similarities with HIPPA, the Federal law which requires group health plans to protect participant personal information.
  - HIPPA is administered through HHS which announced in 2020 eight recent settlements in data breach cases in the millions of dollars.
- **Federal banking and Securities laws:** SEC recently issued a *Risk Alert* describing the increase in cyberattacks against registered investment advisers and broker dealers that resulted in the loss of customer assets or unauthorized access to customer information in some cases. Risk Alert, Office of Compliance Inspections and Examinations, SEC, September 15, 2020.
- **State privacy laws:** Most states have privacy laws which at least two courts have held are not preempted. These laws vary from state to state, and can target plans, plan administrators, TPAs.
- **Other state laws:** Some courts have permitted state contract or tort actions against plans and plan administrators for unauthorized use of personal information, or actions against TPAs under consumer liability laws

Unanswered Questions

- Open question as to whether a participant has an ERISA cause of action against plan or plan service provider when participant personal information (PPI) is hacked — Is the PPI a plan asset?
- Open question as to whether a plan is liable when PPI or plan assets are misappropriated if plan and service providers' cybersecurity measures are prudent.
- Open question as to whether ERISA preempts state privacy laws as applied to an ERISA plan, including state law notice requirements.
- Open question as to whether a plan participant may bring ERISA and state law claims simultaneously.
- Open question as to whether the plan is responsible for participant mistakes or participant carelessness with PPI which leads to a loss.
- Open question as to whether and when TPAs will be vulnerable to ERISA claims by plans or plan participants, and/or state law claims.

Takeaways

- Cyber attacks on retirement plans are increasing, both data hacking and theft of plan assets from participants' accounts. Where service providers or plans used to reimburse participants for hacked accounts, now some are resisting.
- The ERISA law in this area is in its infancy and can only offer precautions by example. Is there a trend toward joint TPA/Plan liability, and a relaxed standard for proving harm?
- Is there a trend toward allowing state law claims in both data hacking and account theft cases?
- Even without specific DOL guidance, ERISA plan administrators and other fiduciaries are responsible for determining appropriate cybersecurity policies and protocols.
- Plan Insurance is an increasingly important consideration.

Best Practices for Plan Administrators

Best Practices

Increasing threat of cybercriminality to retirement plans means plan administrators should review the following steps:

- Insure that on a continuing basis, the plan and all of its service providers who have access to PII are following what are considered the prevailing standards for cybersecurity in the industry. Consider using 1.) multifactor authentication, including encryption, 2.) programs that identify and disable automated scripts used in cyber attacks, 3.) monitoring such as for a higher-than-usual number of login attempts over a given time period, and unusual withdrawal requests in size or frequency.
- Review service agreements any plan service provider with access to PII to ensure there is (1) an agreement to implement and follow plan-specified standards of cybersecurity, including an agreement as to how and when the plan will be notified in the event of a data or asset breach, (2) a commitment to maintain cybersecurity insurance at a particular level, (3) indemnification of the plan for losses, damages, expenses and lawsuits arising out of unauthorized access to participant data or accounts, and (4) adequate representations and warranties.
- Review the plan's fidelity bond to ensure coverage is sufficient for the potential risks involving plan employees who handle plan assets.

Best Practices

- Consider acquiring cybersecurity insurance.
- Review fiduciary liability insurance to determine coverage for fiduciary breach claims, including selection and retention of plan service providers.
- Review of participant data that is currently shared to ensure the minimum possible amount of data is shared.
- Internal training with respect to cybersecurity risks for all individuals who have access to PPI.

Cyber Liability Insurance
Why it Can Matter

What is Cyber Liability Insurance?

Cyber insurance policies generally contain both first-party and third-party coverage. Insures against:

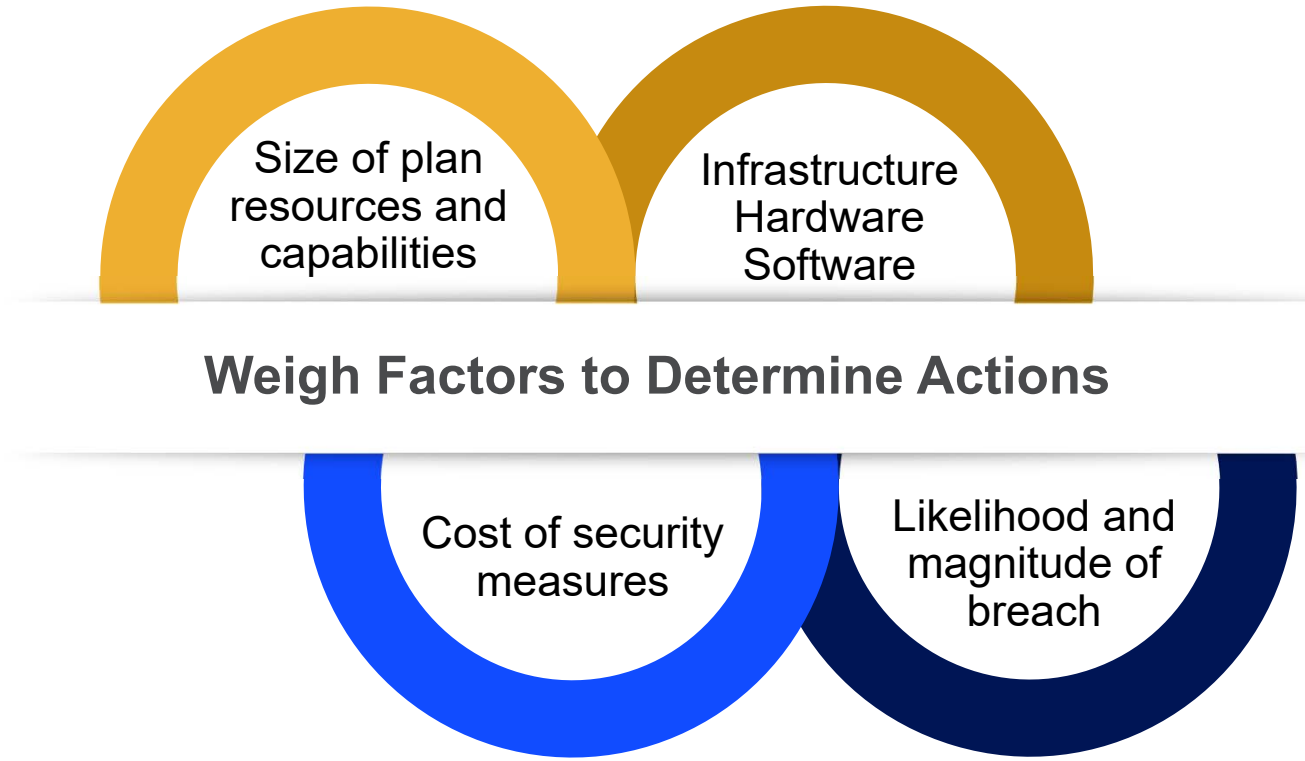
First-Party Coverage

- Insured's own losses, expenses associated with unlawful entry into their computer systems or network as well as breaches arising out lost/stolen devices
- Including the cost to notify insureds of a cyberattack or lost business income
- It should include coverage for ransom payments and extra expenses arising out of cyber extortion

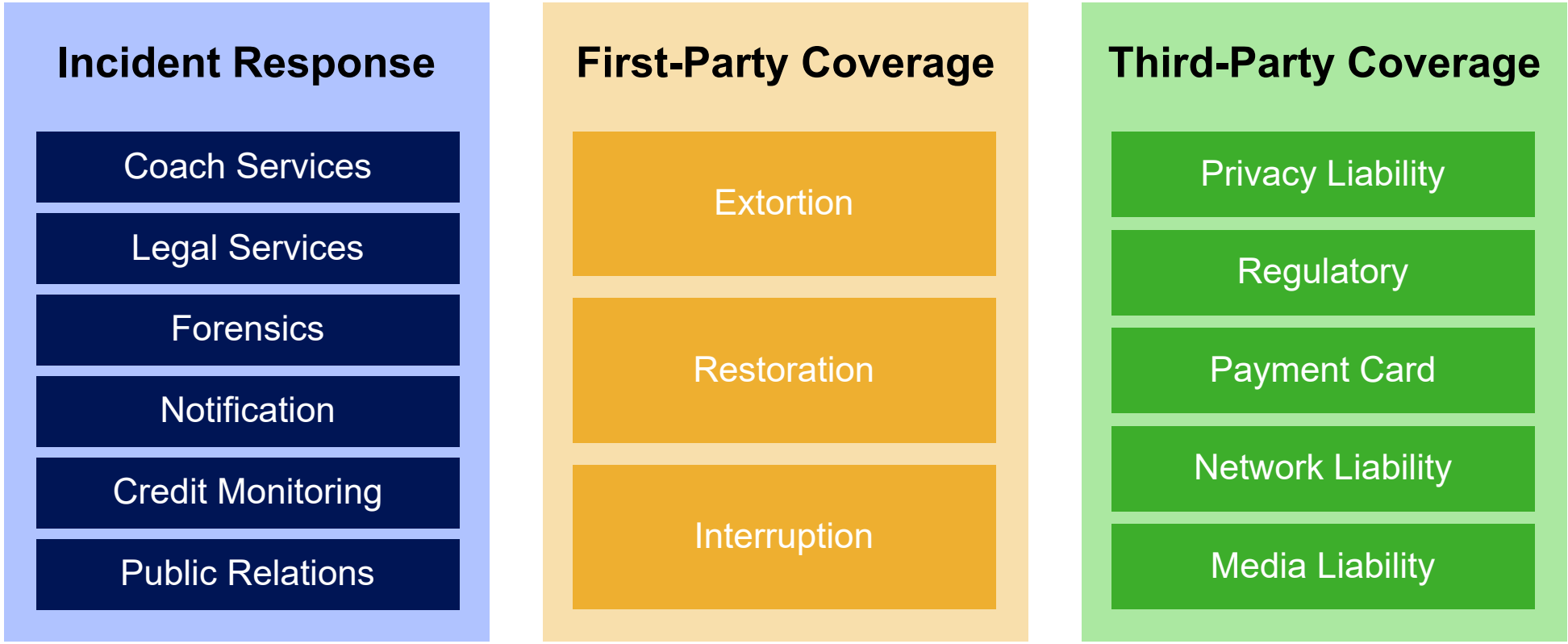
Third-Party Coverage

- Liability to third-parties caused by a breach or cyberattack

When Your Budget is Limited…



Navigating a Data Breach Event

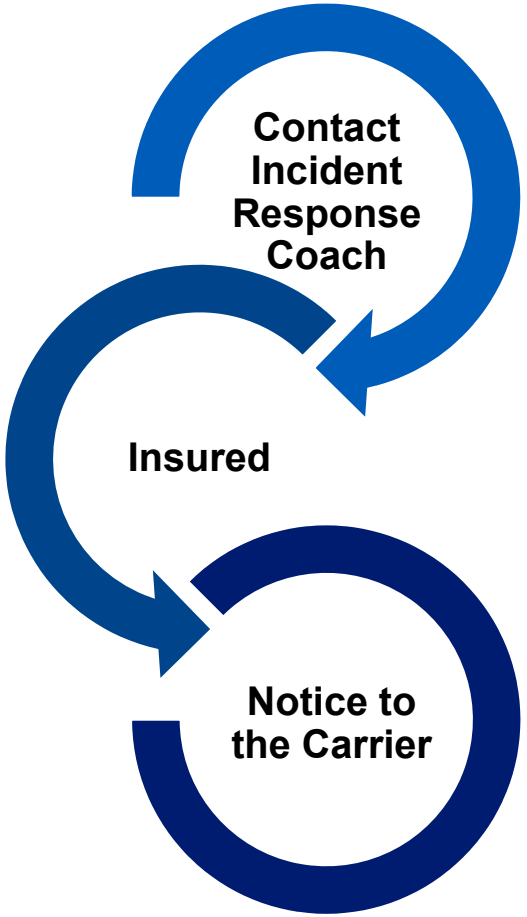


Navigating a Data Event

Incident Response Process Overview

Engage Event Response Team

- Forensics
- Legal
- Crisis Management
- Notification and Call Center
- Credit Monitoring
- Public Relations



Claims set up and Claim Adjuster Assigned

Navigating a Data Event
Engaging the Incident Response Team

Privacy Counsel and Claims Specialist will help formulate your response plan:

- Engage pre-approved expert privacy attorneys to determine legal applicability of actions to respond to reporting requirements and maintain privilege
- Engage computer forensics to determine existence, cause and scope of the breach.
- Do we need to hire a public relations or crisis communications firm?
- Do we need to notify? If yes, who? Customers? Employees?
- Do we need a call center?
- Do we need to provide credit or identity monitoring?

Navigating a Cyber Policy

- Coverage grants are often labeled differently
  - Lack of uniformity
- The policy terms should be reviewed annually for updates
  - Coverage is changing constantly as product develops
- Cybersecurity vendors can vary by carrier
  - Flexibility to choose vendors varies, as well
- Should not purchase cyber coverage based on price alone

Coverage Concerns in a Remote Environment
Ransomware Attacks

- Attacks continue to increase in their frequency and in their ruthlessness
- Often let in by insiders who have been trained not to do so
- The opportunities for a successful attack have increased in the Covid environment:
  a. more distributed access points such as home computers, cell phones and tables
  b. fewer integrated controls on employee-owned computers
- How big of a problem?

  "Beazley Breach Insight: Ransomware rises 25% in Q1 2020

  Phishing scams soar as cyber criminals manipulate COVID-19 uncertainty"

  https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html

Insurance for Ransomware Attacks

Attacks are generally covered by most carriers but the extent varies:

- May employ forensic and other experts to thwart the attack in real time
- May provide professional negotiators to engage the attackers
- May pay the ransom up to a sublimit
- May provide payment via an electronic currency
- May cover extra expenses incurred during downtime to continue critical operations
- May cover damage to data or equipment as a result of the attack

Coverage Concerns in a Remote Environment

Social Engineering is the art of manipulating the target into providing confidential/personal information or transferring assets through:

Phishing	Pharming
Pretexting	Social Media

Decreased co-worker interaction, greater dependence on technology, increased distractions at home, and reliance on email instead of face-to-face communication with colleagues all exacerbate the problem.

Coverage Concerns in a Remote Environment

Social Engineering Fraud

- Attacks are generally covered by most carriers when malware is added, data is stolen or held hostage, or money transferred
- The coverage may have exclusions and require certain procedures to be followed in order to have a covered claim (independent call back provisions, etc.)
- If money is stolen, coverage limits are often sublimited to between $50K and $250K regardless of the full policy limit
- There may be similar coverage in other policies such as a fidelity bond
- Larger coverage limits are usually only available by having excess carriers participate in a program

Beware of Cyber Policy Exclusions

- Professional services
- Criminal or Intentional acts of employees
- “Failure to Follow Minimum Required Practices”
- Acts prior to the inception of the policy
- Unencrypted data exclusion
- Mechanical/electronic failure such as when a computer stops functioning
- Laptops and other portable electronics such as cell phones and tablets
- Patent, software, copyright Infringement
- War or Terrorism

Applying for Cyber Liability Insurance

How many employees have access to data?

Is there an breach response plan in place?

Is there ongoing security training?

Who's responsible for data security?

Is there an information security policy and how are violations handled?

What has the breach experience been and how handled?

Are there contracts in place for 3rd parties who process, host or store sensitive information?

Takeaways

- Ransomware attacks are increasingly focused on retirement plans and are costly
- Social engineering attacks are becoming more sophisticated, harder to detect, and expensive
- Ensure that essential business functions receive the highest focus and effort (e.g., pension distribution)
- Review your cyber liability insurance to make sure your organization has the right type and level of coverage
- Continuously train your staff to employees to avoid common mistakes

Summary

- There are increasing instances of cyber breaches with the increasing use electronic means of plan disclosure and plan asset transactions.
- The federal and state law is developing but not certain.
- ERISA compliance by plan administrators is measured by the plan's cyber policies and protocols based on prevailing expert standards.
- A Plan's cyber policies and protocols should be applied to every person and entity that has access to PII and monitored to ensure the cyber policies and protocols are followed.
- Consider your plan's insurance coverage.

Thank You!

Stephen Wilkes and Susan Rees
The Wagner Law Group
202-969-2800
SWilkes@wagnerlawgroup.com
SRees@wagnerlawgroup.com

Diane McNally
Segal
Senior Vice President and Principal
212-251-5146
drmcnally@segalco.com