Plan Sponsors Growing Fiduciary Responsibilities for Cyber Security

SPARK Institute National Conference June 1-2, 2017

Greta E. Cowart

Winstead PC
Shareholder
2728 N Harwood Street, Suite 500
Dallas, TX 75201
gcowart@winstead.com
214-745-5275

Wendy Y. Carter

Segal
VP, DC Director & Public Sector
1800 M Street NW, Suite 9005
Washington, DC 20036
wcarter@segalco.com
202-833-6422

WINSTEAD

“The law can’t be right if it’s 50 years old, like, it’s before the internet.”

Larry Paige speech comment at a Google developers conference in 2015 (punctuation added)

- If laws cannot keep up with technology, litigation will fill the gaps and contractual protections must fill gaps
- Nearly all states have enacted breach notice laws
- Employers receive much of the data provided to retirement plan record keepers first as employers so the data may be protected by obligations on the:
  - Employer
  - Plan sponsor, or
  - Plan fiduciary
- State laws applicable to employers requiring SSN protection
- AICPA Audit Initiative to review management control of cybersecurity

Cyber Security – Good Business Practice

- Association of Corporate Counsel issued Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information January, 2017
- Expectations for Outside Vendors
- Approach for setting expectations
- AICPA – Risk Management Framework for cybersecurity reporting by management, April 2017
- SOC 1 and SOC 2 and ISAE3402

Cyber Security Potential Risks

- Reputational damage
- Loss of intellectual property
- Disruption of business operations
- Fines and penalties governments assess
- Litigation and remediation costs
- Exclusion from strategic markets
- Damage to employee relations for an employer or to a client's relations with its employees
- Increased legal and cyber insurance costs
- Costs to mitigate damages
- Loss of customers/clients

Cyber Security Risk

- Not if, but when breach occurs
- Breach can come in many forms
  - Malware
  - Ransom ware
  - Phishing
  - Hacks
  - Employee missteps and oversights
    - Sent employee data spreadsheet home to be made pretty
    - Left laptop or flashdrive on public transit
    - Employee posts employee census not using secure file transfer protocol but on company website

Cyber Security for Benefit Plans

- Began with HIPAA Privacy and Security requirements for health plans beginning in 2002 and 2003 for the privacy requirements and in 2004 and 2005 for the security requirements
- HIPAA Security framework of obligations provides a structure which may be used as a starting point for security and risk assessment for cybersecurity, but remember it was developed for 2004 and 2005

Basic Regulatory Cyber Security Structure

- Standards for Security
  - Physical
  - Administrative
  - Technical
- Service Provider Standards
- Notice
- Record Retention
- Breach Procedures
- Responsible Officials

Cyber Security and Trust Law

- Restatement of Trusts – trustee has the duty to protect trust property from loss or damage and has a duty of loyalty which requires the trustee to preserve the confidentiality and privacy of trust information from disclosure to third party except as required by law or necessary to proper administration of trust.
- Retirement plans have trusts and some welfare benefit plans have trusts

Cyber Security for Retirement Plans

- Plan sponsors must consider risks under:
  - ERISA
  - State laws
  - Private rights of action recognized in case law
  - Reputation risk
  - Increasing focus by federal agencies
  - EU Data Privacy

Cyber Security & Plans

- ERISA – Electronic Disclosure Requirement: DoL Reg § 2520.104(b)-1(c)
  - Issued in April 2002 before many of the new technologies
- To use electronic disclosure of plan documents to satisfy a plan administrator's or a fiduciary's obligation to furnish documents to an individual, the plan administrator must, among other requirements:
  - Ensure that the system furnishing documents…

    "Protect[s] the confidentiality of personal information relating to the individual's accounts and benefits (e.g., incorporating into the system measures designed to preclude unauthorized receipt of or access to such information by individuals other than the individual for whom the information is intended);"
- ERISA Technical Release No. 2011-03

Consequences of Failing to Satisfy Electronic Delivery Requirements for a Defined Contribution Plan

- Failure to provide a participant in a DC plan with quarterly or annual account statement an up-to $110 per day per person and per document (502(c)(1))
- ERISA Reg. § 2550.404a-5(a) – requires plan administrator to "ensure that such participants and beneficiaries on a regular and periodic basis, are made aware of their rights and responsibility with respect to the investment of assets held in their accounts and are provided sufficient information regarding the plan, including fees and expenses, and regarding designed investment alternatives – to make informed decisions with regard to investment of their accounts"
- If plan administrator does not comply with the disclosure requirements, and disclosure does not meet the requirements in 2550.404a-5(a), then the duty to disclose is not satisfied, the participant has not exercised control, and participants are not allocated investment responsibilities and the investment of such accounts and related fiduciary duties fall back on the plan fiduciary

Cyber Security

- Plan administrators need to preserve security of retirement plan information to be able to use electronic delivery of documents and information to participants DoL Reg § 2520.104b-1(c)
- Failure to deliver participant quarterly and annual account statements from a defined contribution plan can result in an up-to $110 per day per document per participant civil monetary penalty (502(c)(1))
- Failure to provide blackout notices or the notice of the right to diversify from an investment in employer securities may result in a penalty of up-to $133 per day per participant (502(c)(7)) (adjustment to penalty effective 1-13-17)
- Failure to provide information on investment alternatives means not all requirements for the 404(c) relief for fiduciaries will be satisfied

Loss of ERISA 404(c) Protection

- Fiduciary no longer relieved of fiduciary duties with respect to participant investment selection
- ERISA actions for breach of fiduciary duty:
  - Re: Selection
  - Re: Monitoring
  - Re: Failure to remove
  - Re: Fees
- ERISA Civil Penalties for failed Blackout Notices or Diversification Notice not delivered effectively and electronically of up-to $133 per day per participant
- Fiduciary now exposed to additional breach of fiduciary duty claims from participants

Consequences of a Failed Electronic Notice Under ERISA

- Your ERISA notice is not treated as made
  - QDIA – loss of protection for plan fiduciaries for placing funds in QDIA (404(c)(5))
  - SOX notice (blackout notice) loss of protection for plan fiduciaries and civil monetary penalties (101(i))
  - Change in investment alternative or for participant directed investments (404(c))
- Loss of these notices due to breach in the confidentiality of personal data for the retirement plan participants means the electronic notice may not meet the requirements for the plan fiduciaries to be able to avail themselves of the benefit of the relief under ERISA and liability and potential civil monetary penalties for some notices

IRS Electronic Notice Requirements Treas. Reg. 1.401(a)-21

- Only applies to IRS-required disclosures
- May permit electronic elections
- 2 ways to do IRS disclosures electronically
  - With participant consent (which can be withdrawn)

    or
  - With effective ability to access and free paper copy of applicable notice
    - Must be an electronic medium that the recipient has the effective ability to access
    - *System must preclude someone from making an unauthorized access*
    - System must give the participant an opportunity to review, confirm or rescind an election
    - Participant elections and spousal consents must be witnessed

IRS Electronic Notice Requirements Treas. Reg. 1.401(a)-21

- IRS electronic disclosure rules only apply to IRS-required disclosures for retirement plans and for
  - Code Sections 104(a)(3), 105, 125, 127
  - Qualified transportation fringe under Code Section132
  - Archer MSAs (220) and HSAs (223)
- IRS-governed electronic disclosures and elections
- IRS electronic disclosure and election rules do not mention protecting security or confidentiality – only precluding unauthorized access
- Loss of delivery of 401(k) safe harbor notices
- IRS rules do not apply to ERISA Title I or IV notices or disclosures for suspension of benefits under Code § 411(a)(3)(B) or COBRA notices

What Data do Retirement Plan Vendors Have?

- Name
- Address
- SSN
- Beneficiary and their information (Name, SSN, Address)
- Spouse (information)
- Compensation
- Account Information
- Transaction Information
  - SPARK Institute is undertaking to develop recordkeeping industry standards for data security (Investment News Article 7-21-2016)
  - Employers have risk due to their selection of, and duty to, monitor plan service providers (*Tibble v. Edison Int'l, Inc.*, 135 S.Ct. 1823 (2015)) and *George v. Kraft Foods Global Incorporated*, 641 F.3d. 786 (7th Cir. 2011))

Loss of Protection of Personal Data

- Potential violation of international data protection laws or triggering international data breach notification laws
- Potential FTC Act violation and deceptive trade practice charge for violation related to use or mining of data
- State law and common law based actions for inappropriate disclosure of private info or for a violation of right of privacy
- Cost of identity theft protection
- EU Data Privacy
- Cost of Future Cyber Security Insurance

Loss of Protection of Personal Data

- Corporate reputation damage – big breaches get publicized (e.g., Yahoo)
- Record Keeper reputation damage
- Plan sponsor's risk as employer - state law exposure for not protecting the employees' social security numbers in many states
- Restoration of plan benefits and earnings taken by cyber thieves through breaches and potentially no insurance protection since most fiduciary insurance policies do not pay for benefits
- Impact on premium for cyber security insurance for plan sponsor and for record keeper
- Plan sponsor's risk as fiduciary
- Plan sponsor's risk due to failure to provide required notice

Retirement Plan Cyber Security Protection

- 2016 ERISA Advisory Council Report on Employee Welfare and Pension Benefit Plans included cyber threats as a critical risk to be managed by plan sponsors and vendors
- Consider loss prevention and data security
  - File transfer and file transfer protocols
  - Encryption
  - Data protection through security monitoring for threats
  - Secure websites
  - Cyber security insurance
- Employer's goal is to avoid being the next weak link a hacker finds
- Protect plan fiduciaries and help them protect participants' and beneficiaries' personal information to avoid claims

Commonly Used Security Framework Reminder

- Risk Assessment
- Confidentiality Requirements
  - Administrative
  - Physical
  - Technical
- Permitted Disclosure or Use
- Notice
- Training and Retraining
- Breach Response and Reporting
- Breach Notification
- Mitigation of Harm
- Remedy
- Bind Vendors

Government Framework for Security

Government framework provides a basic structure, but –

- Fails to plan for potential litigation risks the employer may face
- Fails to consider the need for public relations and correct outreach efforts to:
  - Impacted individuals
  - Government agencies
  - Press
- Fails to consider impact to corporate image
- Fails to consider contractual notice requirements
- Fails to contemplate cyber insurance
- Fails to consider other laws
- Does not identify way to accomplish security goals in any particular system

Government Framework Provides Basic Structure But -

- Does not address what to do when violating party cannot be sanctioned or terminated (e.g., cannot terminate vendor without notice or problem is another vendor)
- Does not address what to do if service provider sends data to another country for processing data and issue is abroad where employees cannot be terminated

Retirement Plan
Data Security Steps

- Due diligence on vendors needs to consider security of systems, practices and procedures, data and facilities and breach procedures
- Review requirements on software, physical and IT system operations and system security and monitoring with an IT professional
- Vendor cyber security insurance
- Agreements
- Vendor requirements for employee screening
- Protect the personal information by contract
- Be prepared to demonstrate that you considered data protection for the retirement plan

Security and Vendor Contracts

1. Confidentiality of information requirements and define how data can or cannot be used or mined
2. Data security compliance – which laws or standards
3. Data protection protocols and standards and procedures, e.g., tracking frequency
4. Security incident procedures and notification procedures
5. Limitations of and Exclusion from liability
6. Security or Process Audit standards – SOC1, SOC2, ISAE 3402

Security and Vendor Contracts

Background checks of personnel

Obligation to notify Plan Sponsor of a breach (or duty to promptly investigate suspicious facts)

Obligation to mitigate damage from a breech

Cyber security insurance? Terms? Parties protected? Copy of policy?

Subject to federal cyber security regulation? Provide a copy of compliance program

Cyber Security Starts and Ends with People

1. Who handles cyber security?
2. What procedures must they follow?
3. How are they trained?
4. What procedures or policies exist to guide the staff?
5. On what equipment will persons be able to access data?
6. File transfer protocol?
7. Who must have access to the data?
8. Plan sponsor’s cyber security management plan and tracking?
9. Device control?
10. Disciplinary policies (watch for CBA restrictions)
11. State law or other restrictions on data transfer use?

Implement the Plan; Transfer the Remaining Risk

- **Several proposed "best practices"**
  1. Identify the risk issues via a Risk Assessment
  2. Eliminate or minimize the risk
  3. Preplan an Incidence Response Plan
  4. Test the plan
- **Consider risk transfer**

Without adequate controls, you may not be able to get the insurance protection that is needed

Cyber Liability Insurance Coverage in Action

- It's not just the expense and liability coverage…
- It's the event management capability!

Segal Select Insurance 28

Cyber Liability Insurance

- Partial to full risk transfer that risk assessments and IRPs do not eliminate
- Experienced professionals (legal, forensic, PR)
- Data-packed web sites to help create a robust internal control environment
- 1st party coverage not available elsewhere
- 3rd party liability relating to data breaches

Segal Select Insurance 29

Covered 1st party costs

- Legal
- Forensics
- Public Relations/Crisis Management
- Notification
- Call Center Operations
- Credit Monitoring
- ID Theft Resolution
- Other potential expenses

Experts:
Legal, Forensic, Public Relations

Segal Select Insurance 30

3rd Party Liability Also Included

- Liability concerns:
  - Privacy liability
  - Network security liability
  - Internet media liability

- Triggered by a claim:
  - Against the plan or its trustees or employees
  - By a 3rd party such as a participant or a regulatory body
  - Provides cost of defense
  - Provides indemnification for settlements and judgements
  - Covers fines and penalties where insurable
- Coverage can overlap with fiduciary liability insurance; more important if fiduciary coverage in not purchased

Segal Select Insurance 31

Applying for Coverage

- Approximately how many personal records are stored and how are they stored?
- How many employees have access to data? Is there regular training of employees? Has responsibility for data security been assigned to any one individual such as a CISO?
- How large is the Plan?
- Does the sponsor have an incident response plan? Is it tested?
- Does the sponsor have an information security policy? How are violations handled?
- Does the sponsor use 3rd parties to process or store sensitive information?
- Has the sponsor experienced a breach incident in the past 2 years?

"No" answers could result in higher premiums, not necessarily declinations

When Bad Things Happen

- Data Protection – Identity Theft Protection
- Breach Response
  - Who do you call?
    - Legal Counsel
      - Notification Obligations
        - State Law Notice
        - Contract (CBA)
        - Insurer
        - Affected individuals
      - Laws violated
        - Federal (disclosures to affected individuals)
        - State protection of PII
        - EU
        - Fiduciary obligations
      - Initiate investigation in anticipation of litigation
        - identify scope of breach
        - identify potential impact
        - identify potential cause

When Bad Things Happen

Who do you call?

- Head of IT Department
  - What happened?
  - How did it happen?
  - How can we prevent recurrence?
  - What was acquired or compromised?
  - What must be done to mitigate harm?

What do you tell the IT department to do?

- Investigate
- Determine who are the impacted individuals or entities
- Do no discuss their findings with anyone other than the GC or outside counsel

When Bad Things Happen

Who do you call?

- GC or outside counsel and he/she calls:
  - Cybersecurity Insurance Carrier
  - Public Relations
    - What message?
    - Who tells?
    - Who is told and when?
  - State law breach reporting
  - Contact and contract with identity theft monitoring service
- GC/outside counsel – litigation hold – should it be issued?
- GC/outside counsel – identify disclosure strategy and timing
- GC/outside counsel – how will this be communicated to investors in light of overall risk management? Efforts were communicated to investors?

When Bad Things Happen

Which government agencies might need to be contacted?

- ICC3
- US-CERT
- Secret Service
- FBI
- Local Police
- FTC deceptive trade practices

Other Risks

- If some employees from EU and their data is transferred to the US, there is a risk of violation of EU Data Privacy or pending EU General Data Protection Regulation – GDPR
- If some employees from UK, initial risks in violation of EU data privacy and then post-Brexit effective date, the new UK data privacy
- If US data processed in other jurisdictions, understand security in other jurisdictions and their ability to sanction employees in those jurisdictions
- Remember security depends on people – selecting, training, guiding with mandated policies and procedures, addressing missteps

The following slides contain additional data and resources and are provided as supplements to the presentation.

Increased Focus on Cyber Security

- NIST framework for Improving Critical Infrastructure Cyber Security issued in 2016 to assist companies in evaluating their own security
- Why Retirement Plan Security?
  - State laws 48/50 have enacted data breach laws -See National Conference of State Legislatures website at:
    - http://www.ncsl.org/telecommunications-and-information-technology/security-breach-notification-laws.aspx
  - Employer's Risk for Breach of State Law Privacy Rights
- Risks Under ERISA
- Other Employer Risks
- State laws protect more personal information than just health information and are generally not directed at or attempting to regulate benefit plans

Other Potential Federal Privacy Regulations

Gramm-Leach-Bliley Act – P.L. 106-102

- Generally applies to “financial institutions” (banking, securities and insurance)
- May not apply to all recordkeepers
- Requires federal bank regulators, the NCUA, Treasury, SEC and the FTC after consultation with the representatives of state insurance authorities designated by the NAIC, each to prescribe regulations to carry out the GLB privacy provisions
  - Notice to consumers and disclosure
  - Third party opt-out requirement rules
- Enforcement of GLB privacy requirements by federal regulators and state insurance regulators and FTC
- FDIC, Federal Reserve and the Office of the Comptroller of the Currency announced project to start regulatory process on cyber security standards for large financial institutions

Retirement Plan Cyber Security Protection

- FTC has a mandate to regulate cybersecurity under § 5 of the FTC Act which prohibits unfair or deceptive business practices in or affecting commerce. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) affirmed the FTC's authority to regulate cybersecurity
- FTC is using its authority to pursue actions to protect data security
- Financial Institutions have certain privacy obligations under Gramm-Leach-Bliley Act
- If record keeper is not a financial institution, the law may not provide protections and plan administrator/fiduciary may want contractual protections for plan participants and themselves.

Increased Focus on Cyber Security

- The employer has the data for the retirement plan and often feeds it to the record keeper
- Record keepers are largely not regulated, financial institution regulators have new cyber security regulation in process
- Not applicable to all record keepers
- FTC is pursuing cyber security failures as a deceptive trade practice
  - Memo regarding data use and HIPAA
  - Litigation regarding data security

Increased Focus on Cyber Security

- National Cybersecurity and Communications Integration Center (NCCIC) within Department of Homeland Security
  - Sharing information on cyber threats between private sector government and international network defense communities
  - Shared situational awareness
  - Orchestrating synchronized response
- United States Computer Emergency Readiness Team (US-CERT) – 1 of 4 NCCIC departments
  - Report cyber security incidents to US-CERT
  - http://www.us-cert.gov/report
  - Federal Information Security Modernization Act of 2014

2014 FBI Internet Crime Report

- Over last 5 years, the FBI's Internet Crime Complaint Center ("IC3") averaged nearly 300,000 complaints per year

  or 22,000 complaints per month
- 3,175,611 complaints have been reported to IC3 since its inception May 2000
- Complaints can be filed at www.ic3.gov

Internet Crime Reporting

- IC3 aggregates related complaints to build cases and referrals to local law enforcement
- 2014 Complaints – 269,422
- 2014 Total Losses Reported – $800,492,073
- 2014 Average Dollar Loss

  for Complaints Reporting a Loss – $6,472
- Social media is being used in identity theft
- How many of your employees/plan participants are on social media?

Breach Reports

- 47% of breaches discovered by victim, 53% via third party notification
- 146 : is the median days between breach and discovery
- Business disruption attacks increased
  - Ransomware
  - Malware, Cryptolocker
  - Destruction of critical data
  - Publication of sensitive data
  - Theft of funds
- Chinese hackers
- Russian malicious cyber attack – GRIZZLY STEPPE – Dec. 29-30, 2016
- APT – advanced persistent threats – Russian hackers
- 2 types of companies – those that knew they have been hacked and those that have been hacked

Questions?

Thank you for your attention.

Greta E. Cowart

Winstead PC
Shareholder
2728 N Harwood Street, Suite 500
Dallas, TX 75201
gcowart@winstead.com
214-745-5275

Wendy Y. Carter

Segal
VP, DC Director & Public Sector
1800 M Street NW, Suite 9005
Washington, DC 20036
wcarter@segalco.com
202-833-6422