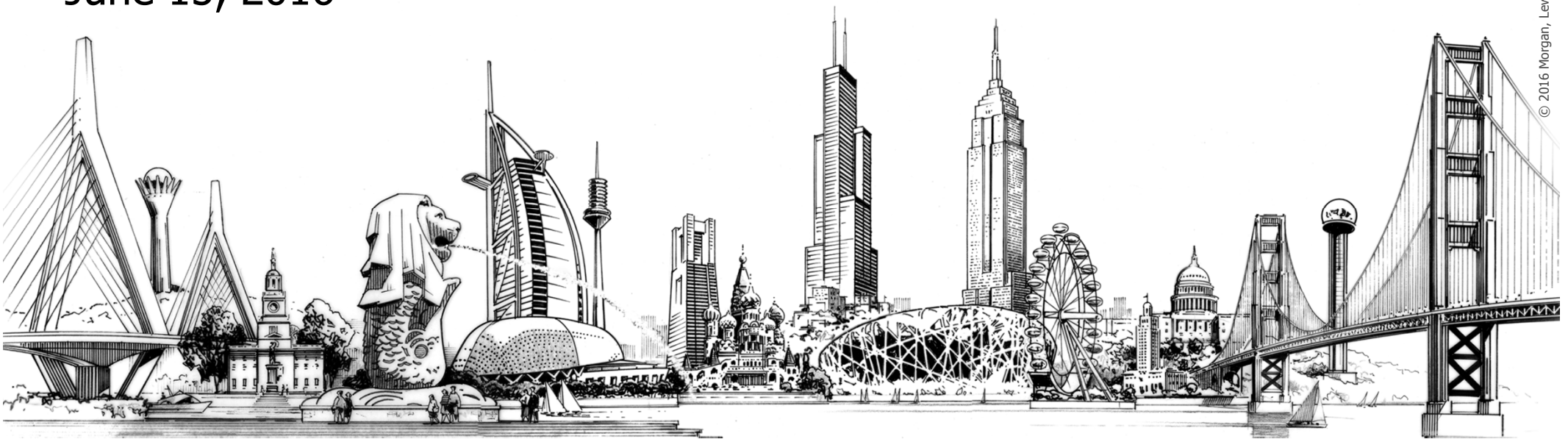
Morgan Lewis

DATA PRIVACY AND CYBERSECURITY FOR RETIREMENT PLANS AND PLAN FIDUCIARIES: ARE YOU AT RISK?

Presenters: Kristin Hadgis, Matthew Hawes, and Patrick Rehfield

June 15, 2016



Overview

- Why you should care about data privacy and cybersecurity
- Why this impacts plan fiduciaries
- How you should manage your fiduciary responsibilities
- Some practical tips and lessons learned
- Where we see data privacy and cybersecurity in the future
- Discussion of some real-world recent examples of breaches and steps that could be taken to help keep these from happening to you

Privacy Landscape: Data Privacy and Cybersecurity Should Be a Priority

- Privacy continues to dominate headlines and top worries of corporate executives
- Recent statistics/studies:

In 2015:

781 breaches

affecting

more than 169 million records

Source: Identity Theft Resource Center

Privacy Landscape: Data Privacy and Cybersecurity Should Be a Priority

- Recent statistics/studies (cont.)

  Average cost per breach:

  $3.4 million (direct and indirect costs)

  --

  $154 per record

Source: Ponemon Institute and IBM

- Private litigation continues and may be gaining traction

Privacy Landscape: Data Privacy and Cybersecurity Should Be a Priority

- Sample of 2015 Breaches
  - Large Health Insurer: Database hack obtained personally identifiable information for 78.8 million individuals, including names, dates of birth, Social Security numbers, healthcare ID numbers, home addresses, email addresses, and employment information, including income data.
  - Larger Health Insurer: Compromise of the names, birth dates, email addresses, and subscriber information for the 1.1 million members, but member password encryption prevented cybercriminals from gaining access to Social Security numbers, medical claims, and employment, credit card, and financial data.

Privacy Landscape: Data Privacy and Cybersecurity Should Be a Priority

- Sample of 2015 Breaches (cont.)
  - Credit reporting agency hack affecting cell phone customers: According to the company, the breach occurred from September 1, 2013 to September 16, 2015 and resulted in stolen data of 15 million cell phone customers, including names, birth dates, addresses, Social Security numbers, and drivers' license numbers.
  - Office of Personnel Management (OPM): Announced in June 2015, this second OPM breach affected the background investigation records of current, former, and prospective federal employees and contractors and included the Social Security numbers of 21.5 million individuals.
  - Hotel Chain: Between May 19, 2014 and June 2, 2015, malware exposed the credit card information (including account numbers, expiration dates, and security codes) of customers at a number of the hotel properties in the United States and Canada. In April 2016, the hotel chain disclosed a potential new data breach likely affecting customer credit card data.

Data Privacy and Cybersecurity for Plan Fiduciaries

- Retirement plans are an extensive source of valuable personal data about participants and beneficiaries
  - Social Security numbers
  - Addresses
  - Dates of birth
  - Bank account information, etc.

  This collection of information presents an attractive and potentially exploitable opportunity for criminals.

Privacy Landscape: Data Privacy and Cybersecurity Should Be a Priority

- Employee Error Is a Primary Contributor to Data Breaches
  - More than 50% of surveyed companies reported they have experienced a security incident because of a negligent or malicious employee.
  - Key concerns:
    - Downloading malware from website or mobile device
    - Targeted phishing attacks

Source: Experian Data Breach Resolution and Ponemon Institute (2016)

Privacy Landscape: Data Privacy and Cybersecurity Should Be a Priority

- A Media and Social Networking Company Breach
  - The company lost 167 million credentials and passwords in a 2012 hack.
  - In May 2016, the email addresses and passwords were again offered for sale on a dark web marketplace for five bitcoins (about $2,300)
  - Breach connected to recent phishing efforts targeting customers

Privacy Landscape: Data Breach and Cyber Threats

- International hacking groups
- Cyberespionage
- State-sponsored intrusions
- Cyberfraud
- Hacktivists
- Greater sophistication
- Malware

Data Privacy and Cybersecurity for Plan Fiduciaries: Good News/Bad News

- **Good News** – There is no all-encompassing data privacy or cybersecurity statute in the U.S.
- **Bad News** – There is no all encompassing data privacy cybersecurity statute in the U.S.:

Attorney General Enforcement
FTC Act
FCRA
CAN-SPAM
COPPA
Breach Notification Laws
Data Disposal Laws
Gramm-Leach-Bliley
MA Data Security Laws
Red Flags Rule
FACTA
EU "safe harbor" rules
Consumer Class Actions
PCI and DSS Credit Card Rules
Document Retention Requirements
HIPAA

CA Online Privacy Act
Stored Communications Act/ECPA
Do Not Call Lists
Telephone Consumer Protection Act
Video Privacy Protection Act
Wire Tapping liability
Invasion of Privacy Torts
Data Encryption Laws
Identity Theft Assistance
E-Sign
Computer Fraud and Abuse Act
Communications Decency Act
Spyware Laws
RFID Statutes
FDCPA
Driver's Privacy Act
Social Security Number Laws
Regulation Z

****No comprehensive federal law governing data privacy or cybersecurity at the retirement-plan level**

Data Privacy and Cybersecurity for Plan Fiduciaries

- Common misconceptions:
  - *Cybersecurity is an IT problem.*
  - *I am compliant with HIPAA and HITECH; I don't need to worry about these issues.*
  - *I have reputable vendors administering my plans. They store the plan data, so it is their responsibility to worry about these things.*
- Data breaches are real.
- Data breaches are expensive.
- Data privacy and cybersecurity cannot be ignored.

Data Privacy and Cybersecurity for Plan Fiduciaries

- Fiduciary Duty of Loyalty:

  ERISA requires that plan fiduciaries act

  – Solely in the interest of participants and beneficiaries

  – For the exclusive purpose of providing benefits and defraying reasonable expenses

Data Privacy and Cybersecurity for Plan Fiduciaries

- Fiduciary Standard of Care
  - Strict (and high) standard of care – fiduciaries must carry out their duties with the *care*, *skill*, *prudence*, and *diligence* under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a *like character* and with *like aims*
  - This is the so-called prudent expert standard
  - A breach can occur from both action and inaction

Data Privacy and Cybersecurity for Plan Fiduciaries

- *Personal liability* for fiduciary breaches and losses stemming from breaches (no exculpatory provisions)
- Obligation to restore profits
- Other equitable and remedial relief (e.g., removal from fiduciary position)
- Additional penalties
  - Monetary penalties of 20% of recovery amount
  - Criminal penalties for willful violations of reporting requirements or fraud, force, or violence

Data Privacy and Cybersecurity: Managing Fiduciary Responsibilities

- No precise description of what is procedurally prudent under every circumstance
- Go back to standard of care definition:

  "Fiduciaries must carry out their duties with the *care*, *skill*, *prudence* and *diligence* under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a *like character* and with *like aims* . . ." .

Data Privacy and Cybersecurity: Procedural Prudence

- Identify sources of data privacy risk and create a project plan
  - Risk can come from internal and external sources and include both physical and cybersecurity risk
  - Solicit input from key internal and external resources
    - Plan management, legal, IT personnel, recordkeepers, consultants, etc.
  - Review security measures
  - Create a plan that reflects clear goals and obligations

Data Privacy and Cybersecurity: Procedural Prudence

- Prepare plan administration
  - Designate a responsible person
  - Establish written policies and procedures governing the treatment of data and security incidents
  - Conduct internal training for plan management personnel
  - Evaluate fiduciary liability insurance coverage for data breach events (consider separate cyber-insurance policy)
  - Educate plan participants and beneficiaries on privacy and cybersecurity (e.g., shredding unneeded files, password security, phishing)

Data Privacy and Cybersecurity: Procedural Prudence

- Evaluate service providers as part of initial selection and ongoing monitoring
  - Evaluate the track record of plan service providers with regard to information security
  - Evaluate provider selection and certifications
  - Ensure service provider agreements adequately address responsibility and liability with respect to data privacy and cybersecurity
  - Require regular updates from service providers on data breaches and cybersecurity incidents

Data Privacy and Cybersecurity: Procedural Prudence

- Create a comprehensive information and data security breach plan
  - Prepare a breach response plan that includes establishment of a breach response team
  - Ensure that the breach response team liaises with appropriate authorities and affected participants, beneficiaries, etc.
  - Periodically test the information and data security breach response plan

Data Privacy and Cybersecurity: Managing Fiduciary Responsibilities

- Add data privacy and cybersecurity to the list of "perennials"
  - Reports from fund providers and investment managers, key vendors, consultants
  - Review of fund and manager performance, including fees and expenses
  - Review of legal/compliance issues
  - Review of participant issues (usage/trends, complaints, claims/appeals)
  - Review of data security and cybersecurity risks, incidents, responses

****Plan fiduciaries need to be proactive and reactive to ever-changing data security threats**

Plan Fiduciaries: Service Provider Management

- Review existing agreements
- Engage with vendors – negotiate changes, applicable riders
- Consider specific data privacy and cybersecurity provisions when engaging new vendors

Service Provider Agreements – Points for Review

- Identification of information subject to data privacy and cybersecurity provisions
- Level of security to be provided
- Data transfer requirements and restrictions
- Identification of where data is to be stored and restrictions
- Breach response responsibilities
- Reporting of information on other breaches
- Audit (physical, policy, etc.)
- Indemnification and limitations on liability as they relate to data privacy, cybersecurity, and breaches
- Termination provisions regarding destruction and/or return of data

Service Provider Agreements – Common Mistakes

- Failing to include requirement that the service provide notice of a breach.
- Failing to consider use of data for derivatives, i.e., use of personal data in an aggregate/anonymized form.
- Not permitting the right to audit the service provider.
- Not requiring reporting and strict security measures if service provider uses other parties, including cloud storage.
- Trying to overcontract, including too many specifics on how to respond to data breaches, overdefining "personal information," etc.

Service Provider Agreements: Problematic Language

- Example 1: Not enough detail on data privacy and cybersecurity responsibilities.

With respect to any personally identifiable information (PII) Vendor receives under this Agreement, Vendor agrees to (i) safeguard PII in accordance with its privacy policy and (ii) exercise at least the same standard of care in safeguarding such PII that it uses to protect the PII of its own employees.

Service Provider Agreements: Problematic Language (cont.)

- Example 2: Too much detail on responding to data breach. Every data breach is unique and may require a tailored approach. Legal requirements and "market" responses are always in flux.

The following shall be considered recommended actions to address and respond to a security breach: (i) preparation and mailing or other transmission of legally required notifications; (ii) preparation and mailing or other transmission of communications to customers, agents, or others required by applicable law, the Payment Card Industry Data Security Standard (as may be amended) or required or recommended by a governmental authority or agreed to by the parties as a reasonable mechanism for mitigating the breach; (iii) establishment of a call center or other communications procedures in response to such violation (e.g., customer service FAQs, talking points, and training) not to exceed 60 days or such longer time required by law or required or recommended by a governmental authority or agreed to by the parties as a reasonable mechanism for mitigating the breach; (iv) public relations and other similar crisis management services; (v) reasonable legal and accounting fees and expenses associated with Client's investigation of and response to such event; (vi) costs for commercially reasonable credit reporting services not to exceed 24 months or such longer time required by applicable law or required or recommended by a governmental authority or agreed to by the parties as a reasonable mechanism for mitigating the breach; and (vii) all claims for government fines, penalties, and interest imposed by a governmental authority.

Service Provider Agreements: Problematic Language (cont.)

- Example 3: Still not enough detail . . .

Privacy. Vendor will implement and maintain a written information security program that contains appropriate security measures to safeguard the personal information of the Client's beneficiaries, unit holders, shareholders, retirees, employees, directors and/or officers that it receives, stores, maintains, processes, or otherwise accesses in connection with the provision of services hereunder. For these purposes, "personal information" shall mean (i) an individual's name (first initial and last name or first name and last name), address, or telephone number plus (a) Social Security number, (b) driver's license number, (c) state identification card number, (d) debit or credit card number, (e) financial account number or (f) personal identification number or password that would permit access to a person's account or (ii) any combination of the foregoing that would allow a person to log onto or access an individual's account. Notwithstanding the foregoing, "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

The Data Breach Wave – Lessons Learned

1. Data security is never "finished" or "covered"
   - Must be an ongoing commitment
2. Response is often in "real time" (e.g., first notice of breach will be call from credit card company, inquiry from press, call from FBI)
   - Emphasizes importance of preparation and planning
   - Develop a breach response plan

Lessons Learned (cont.)

3. Vendor management issues: breaches in the headlines
4. Don’t ignore the “small” things (e.g., small-dollar vendors, password management)
5. Notice continues to be a challenge. (e.g., multiple state and foreign laws, timing)

Lessons Learned (cont.): Insurance Considerations

- Corporate umbrella liability insurance policies often provide (directly or through a rider) liability insurance for fiduciary activities
- Fiduciary insurance policies
- Stand-alone cyber-insurance policies
- Financial loss policies

Future Landscape: Likely DOL Guidance

- Department of Labor's 2016 Advisory Council on Employee Welfare and Pension Benefit Plans
  - 2011 Advisory Council Report on Privacy and Security Issues Affecting Employee Benefit Plans: In 2011, the Advisory Council issued a report recommending to the DOL that it provide guidance on the obligation of plan fiduciaries to ensure data remains secure and private. The 2011 report also recommended that the DOL develop educational materials and outreach efforts for plan sponsors, participants, and beneficiaries to address issues of privacy and data security.
  - Goal of 2016 Advisory Council: The stated goal for the 2016 Advisory Council's work on privacy and data security is to focus on cyber-risk management for employee benefit plans and offer the DOL draft materials that help plan sponsors understand, evaluate, and protect benefit plan data and assets from cybersecurity risks. (https://www.dol.gov/ebsa/pdf/2016-cybersecurity-issue-scope.pdf)

Future Landscape: Likely DOL Guidance

- Department of Labor's 2016 Advisory Council on Employee Welfare and Pension Benefit Plans (cont.)
  - Meetings held last week (June 7-9) at DOL
  - About a dozen witnesses discussed cybersecurity concerns and recommendations (including from SPARK Institute, Segal Consulting, Marsh, and Kroll)
  - Extensive discussion regarding available insurance, typical limits, differences from fiduciary insurance, and standard contract terms and coverage
  - Discussion on vendor agreements and best practices and developing a list of standard questions
  - Clear that guidance will not address fiduciary responsibilities and whether cybersecurity regulations are preempted by ERISA

Future Landscape: Possible Industry Minimum Standards

- SPARK Institute
  - SPARK Institute announced on May 3, 2016 the establishment of the Data Security Oversight Board, with the goal of developing and marketing uniform data-management standards that are intended to provide a baseline of security across defined contribution plan marketplace.
  - SPARK Institute indicated that the criteria for compliance would be confidential
  - DOL Advisory Council commented on SPARK announcement

Future Landscape: Federal Legislation Possible

- "Data Security and Breach Notification Act of 2015," S. 177 (H.R. 1770):
  - Requires the Federal Trade Commission (FTC) to promulgate regulations requiring the implementation of policies and procedures for the treatment and protection of personal information by nonprofit and for-profit corporations, estates, trusts, and other specified entities owning or possessing such information.
  - Covered entities would be required to provide notification of breaches to the FTC or the Department of Homeland Security (DHS) and the affected individuals.
  - Enforcement authority conferred upon the FTC and state and federal attorneys general.
  - Criminal penalties or fines or imprisonment for up to five years, or both, for concealment of a security breach that results in economic harm of at least $1,000 to an individual.

Future Landscape: Federal Legislation Possible (cont.)

- "Cyber Security Information Sharing Act of 2015," passed in December 2015:
  - Directs DHS to coordinate with other federal government entities to set up procedures and portals for sharing information with the privacy sector
  - Allows privacy companies to share information with government and one another, providing protection from liability for antitrust and other suits
  - Protects privacy by requiring removal of all personal information; requires AG to create policies to protect privacy including (1) limits on time that information can be kept; (2) penalties for government officials that violate restrictions; and (3) notification for personal information mistakenly stored

Recent Examples

- "Spoofing" email sent to human resources employee appeared as if it came from company's CEO and asked for all employee W-2s.
- Break-in at company's office after hours where perpetrator went from workstation to workstation looking for passwords left out in the open or under keyboards. Perpetrator found a password and gained access to the company's system.
- Company hired a vendor to send out tax forms. Vendor used an envelope where employee's Social Security number may have been visible if the envelope were shaken just right.
- Company's vendor operating customer service center stole customer information, such as name, address, and financial account information, and attempted to sell that information.

Biography

Kristin M. Hadgis
Philadelphia
T +1.215.963.5563
F +1.215.963.5001
kristin.hadgis@morganlewis.com

Kristin M. Hadgis represents businesses in complex commercial, class action, retail, and product-related litigation in US state and federal courts, including appeals. She represents clients in a wide range of industries, including financial services, retail, pharmaceutical, and medical devices, with particular emphasis on the unique issues facing retailers and other consumer-facing companies. Kristin also focuses her practice on privacy and data security matters, and regularly advises and represents clients in connection with these issues.

Kristin handles all aspects of litigation, from pretrial motions through trial and post-trial appeals. She represents and counsels clients with respect to privacy and data security laws and related requirements, including the Fair Credit Reporting Act (FCRA), US federal and state Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) laws, the Telephone Consumer Protection Act (TCPA), Federal Trade Commission (FTC) rules, the Securities and Exchange Commission privacy regulations (Reg. S-P), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA).

Biography

Matthew H. Hawes
Pittsburgh
T +1.412.560.7740
F +1.412.560.7001
matthew.hawes@morganlewis.com

Matthew H. Hawes helps clients navigate every aspect of employee benefits, executive compensation, and equity compensation, including the drafting and design of qualified pension and profit-sharing plans, health and welfare arrangements, deferred compensation plans, and employee agreements. He also performs employee benefits due diligence reviews in the mergers and acquisitions context, and he advises companies on regulatory compliance with the US Internal Revenue Code, ERISA, COBRA, and HIPAA.

Previously, Matt was a law clerk for Judge Susan P. Graber of the US Court of Appeals for the Ninth Circuit. He also worked as a tax associate in a New York-based law firm, where he advised clients on US federal tax issues, including the consequences of capital markets transactions, private equity investments, and mergers and acquisitions. In that capacity he represented clients in tax controversy matters before the IRS and US federal courts.

Before earning his law degree, Matt spent more than four years serving in the United States and abroad as an officer in the United States Navy, earning the rank of lieutenant. His duties included service onboard the USS Inchon (MCS-12) as the weapons officer, assistant first lieutenant, and combat information center officer; service with the 5th Battalion, 10th Marines, 2d Marine Division as a naval gunfire liaison officer assigned to Weapons Company, 1st Battalion, 6th Marines, 24th Marine Expeditionary Unit; and service as an artillery liaison officer.

Biography

Patrick Rehfield
Washington, D.C.
T +1.202.739.5640
F +1.202.739.3001
patrick.rehfield@morganlewis.com

Patrick Rehfield focuses on matters related to executive compensation, payroll tax, and employee fringe benefits. He advises private and public companies on designing and implementing nonqualified retirement plans, equity compensation plans, and executive compensation arrangements. He also counsels publicly traded companies on reporting and compliance matters involving the SEC, with a focus on proxy and disclosure issues, executive compensation, and corporate governance. He advises public and private companies on employee benefit issues in mergers and acquisitions, including executive compensation matters for senior management.

Patrick also advises companies of all sizes on the design and implementation of employment agreements, retention agreements, and change in control agreements. He represents senior management teams in leveraged buyouts, and senior-level executives in compensation package negotiations. He has particular experience in the application of sections 162(m), 280G, and 409A of the Internal Revenue Code.

Patrick also maintains an active payroll tax and fringe benefit practice that focuses on corporate and payroll tax audits, penalty abatements, refund claims, IRS ruling requests, and multistate tax and withholding issues.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing
Boston
Brussels
Chicago
Dallas
Dubai
Frankfurt
Hartford
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis

THANK YOU