Welcome

Join the Conversation:
Text HOGANTAYLOR to 22333 once to join.
Using bread crumbs to find your way out

Brandon Long
Practice Leader
Employee Benefits & Executive Compensation

McAfee & Taft
Oklahoma City * Tulsa
“Sleeping in the jungle”

- That’s what this presentation should have been called . . . .
Today’s topics

- New lawsuits and what we can learn from them
- New IRS guidance regarding hardship distributions
- Documentation needed for participant loans
- Current industry trends
New Lawsuits
A “fiduciary” is anyone who:

- Exercises any discretionary authority or discretionary control regarding the management of a plan;
- Exercises any authority or control regarding management or disposition of plan assets;
- Renders investment advice for a fee or other compensation, direct or indirect, with respect to plan money or property; or
- Has any discretionary authority or discretionary responsibility in the administration of the plan.
Fiduciary duties

- **Exclusive Purpose Rule** ("Duty of Loyalty") – solely in the interest of the plan’s participants and beneficiaries (don’t forget – and for exclusive purpose …)

- **Prudent Person Standard** ("Duty of Care") – discharge your duties in the manner of a prudent person with the care, skill, prudence and diligence of a person acting in a like capacity and familiar with such matters (Prudent Expert Rule)
Fiduciary duties (cont’d)

- **Diversify the Plan’s Investments** – to minimize the risk of large investment losses

- **Follow the Plan’s Written Rules** – act in accordance with the provisions of the plan documents that govern the plan (i.e. the master plan, adoption and trust agreements, investment policy statement, loan policy, etc.)
Exclusive purpose

- Solely
- Without conflicts
- Without considering other interests
- Solely means solely
Lawsuit #1 - Tussey v. ABB

- Tussey v. ABB (8th Cir.) (March 9, 2017) (Filed in 2006 in Western District of Missouri)
  - Original judgment = $13.4 million related to recordkeeping allegation; $21.8 million related to bad faith mapping allegation; $13.4 million in attorneys’ fees
  - Alleged violation of loyalty when replaced Vanguard fund with Fidelity Freedom funds - allegedly because higher-priced Fidelity funds helped subsidize other services provided by Fidelity to health and welfare plans and defined benefit plan at little or no cost
Allegations in *Tussey v. ABB*

1) Failure to calculate the amount paid to Fidelity with revenue sharing

2) Failure to determine whether Fidelity’s fee was competitive

3) Failure to negotiate lower fees given the size

4) Failure to prevent subsidization of Fidelity’s other services
What we can learn from *Tussey v. ABB*

- Improper motive = no place for deference
- Improper motive = process may not help
Lawsuit #2 - Fujitsu

- Class action lawsuit filed in the Northern District of California
- More than $1 billion in plan assets during the relevant time
- Committee and its members designated as plan administrator
Allegations in *Fujitsu*

- Alleged fiduciary breaches tied to **excessive fees, recordkeeping, and the components of the company’s custom target-date funds**
  
  - Attorneys compared the Fujitsu plan’s fees with those of about 650 other plans with more than $1 billion in assets - average plan has annual costs that amount to 0.33 percent of assets, according to the complaint; it estimates that Fujitsu’s costs were 0.88 and 0.90 percent for 2013 and 2014
Allegations in *Fujitsu* (cont’d)

- Alleged failure to use the cheapest share class

- Complaint also highlights what it deemed “idiosyncratic” investments in *custom target-date* funds created by investment advisory firm

- “Complaint also highlights a practice that many 401(k) plan participants may not know exists: ‘revenue sharing’ between the company offering the funds and the plan’s sponsor — the employer”
What we can learn from *Fujitsu*

- **Status:** Motion to dismiss denied April 11, 2017

- **Takeaways:**
  1. Monitor recordkeeping expenses
  2. Monitor all fees paid to service providers and make sure fees are reasonable
  3. Investigate lower-cost share classes
  4. Be careful with custom target-date funds
  5. Monitor investments and their performance
Lawsuit #3 - *Patrico v. Voya*

- USDC – S.D. of New York
- Opinion on motion to dismiss – June 20, 2017
Allegations in *Patrico*

- Plaintiffs alleged Voya breached its fiduciary duties and engaged in self dealing
- Alleged excessive fees for investment advisory services offered to 401(k) participants
- Plan allows participants to select their investments from a menu selected by the sponsor
- To give participants access to investment advisory services, sponsor entered into agreement with Voya advisory arm
Allegations in *Patricio*

Voya offers two investment advice programs –

1. a self-service, online program called “Personal Online Advisor”; and

2. a managed account service called “Professional Account Manager.”

- Although Voya offers the programs, Financial Engines Advisors, LLC provides the actual investment advice.
Allegations in *Patrico*

- As compensation for the programs, Nestle pays Voya a “Platform Fee” of $8 per year for each Plan participant with a balance in the Plan, or $7 if the program participation rate exceeds 10%.

- Plan participants who enroll in the Professional Account Manager program also are charged a fee based on the value of each participant’s account, e.g., 50 basis points (0.50%) for the first $100,000 invested, 40 basis points for the next $150,000 invested and 25 basis points for amounts in excess of $250,000 invested.
Allegations in *Patrico*

- Plaintiff elected to participate in the investment advice program and utilized Financial Engines’ services. Plaintiff challenges Voya’s role in the program, in essence alleging that it charged excessive fees.

- Plaintiff alleges that Voya “provides no material services in connection with the advice program, and the only reason for structuring the advice service as being provided by Voya with sub advisory services by Financial Engines is to allow Voya to collect a fee to which it is not entitled.”
Allegations in *Patrico*

- Plaintiff claims that, by structuring the investment advice program this way, Voya and the other Defendants breached their fiduciary duties and engaged in prohibited transactions in violation of ERISA.
Patrico court’s opinion

- Breach of fiduciary duty claim fails – because defendants were not fiduciaries
- Plaintiffs are seeking leave to amend complaint to add allegations of knowing participation in a fiduciary breach
What we can learn from *Patrico*

- Pay attention to things your employees are being sold and/or offered by your providers
- Ask a bunch of questions
- Everyone is looking for additional revenue
- Sales initiatives are in full swing
Lawsuit #4 – *Rhea v. Ritchey*

- Fifth Circuit
- May 30, 2017 decision
- Health plan subrogation decision
- Plan used one document as its summary plan description and written instrument
- Rhea refused to reimburse the plan claiming it did not have an enforceable written instrument
Background in *Rhea* (cont.)

- SPD referred to a separate plan document
- Court held SPD can serve as the written plan document
What we can learn from *Rhea*

- Let’s avoid these kinds of disputes
- Pay attention to what your benefit booklet says
- If it says there is a separate plan document, make sure there is a separate plan document
- Otherwise, adjust the language
- Push back against your network and/or TPA – it’s your responsibility, not theirs

---

*McAfee & Taft*
Lawsuit #5 - *Larson v. Allina*

- Filed August 18, 2017
- Federal district court in Minnesota
- Plans have $2.3 billion in assets
- 47,500 participants
- Alleged failure to reduce expenses
- Alleged failure to scrutinize each investment option
- Alleged “rubber stamp” approval of investments
Allegations in *Larson*

- Allegedly included higher cost investment options in the plans that were detrimental to participants
- Allegedly allowed Fidelity to select its own proprietary funds for the plans, as well as other funds paying fees to Fidelity for inclusion in the plans
- Allegedly failing to use the plans’ high levels of assets to negotiate lower fees for certain funds
- Allegedly failing to use collective trusts or other investment vehicles that could have lowered administrative expenses while providing substantially similar investments
Allegations in *Larson*

- Alleged failure to monitor and control the plans’ recordkeeping costs
- Alleged failure to use the plans’ bargaining power to negotiate lower managed account expenses
- Allegedly maintaining multiple money market funds during a sustained period in which all the money market funds earned negligible or even negative returns
- Allegedly failing to switch higher cost and poorly performing investment options for nearly identical, or similar, cheaper and better performing options available in the market
Allegations in *Larson*

- Allegedly failing to adequately monitor other persons to whom fiduciaries had delegated the management and administration of the Plans’ assets
- Allegedly failing to properly identify fees and expenses charged against individual accounts
- Allegedly failing to properly identify the source of the fees and expenses so charged
What we can learn from *Larson*?

1. Understand expenses
2. Pay attention to plan growth
3. Review and ask questions about investment changes
4. Monitor recordkeeping costs
5. Monitor other fiduciaries
6. Notify participants of plan fees
Bread Crumb
Lightning Round
Prudent person standard

- Substantive prudence
- Procedural prudence
- **Bread crumb:** IPS
- **Bread crumb:** Minutes – how to document decisions and how not to document decisions
- **Bread crumb:** RFPs, benchmarking, fiduciary files, etc.
- **Bread crumb:** Participant communications
Prudent person standards (cont’d)

- **Bread Crumb:** Cyber security – (1) what do you have? (2) where is it? (3) how service provider protecting? (4) implement procedures; (5) consider insurance

- **Bread Crumb:** Timely deposits

- **Bread Crumb:** Trying to pick recordkeeper on your own

- **Bread Crumb:** Trying to pick funds on your own
Prudent person standards (cont’d)

- **Bread Crumb:** Not understanding revenue sharing (consider whether worth the risk)

- **Bread Crumb:** Solely means solely: Not holding friends accountable

- **Bread Crumb:** Pay attention to what employees are being offered/sold

- **Bread Crumb:** Read your plan documents
Diversify plan investments

- Do you know how to pick investments?
- Are you an expert on how to pick investments?
- **Bread crumb:** Importance of fiduciary advisor
- **Bread crumb:** Single stock funds
- **Bread crumb:** Target date funds (beware of reset strategy) (beware of underperformance)
- **Bread crumb:** 404(c)
Follow plan terms

- With respect to compensation
- With respect to eligibility
- With respect to contributions
- With respect to vesting
- With respect to plan loans
- With respect to distributions
- **Bread crumb:** Self correction memos
- **Bread crumb:** Loans/hardships
New IRS
Hardship Guidance
Hardships overview

- 401(k) plan may allow in-service distributions of elective deferrals based on “hardship”

- Two requirements: (1) hardship event; (2) distribution must be necessary to meet that hardship (including lack of other resources)
Six safe harbor events

1) Expenses for medical care previously incurred by the participant, the participant's spouse, or any of the participant's dependents, or expenses necessary for these persons to obtain medical care.

2) Costs directly related to the purchase of a principal residence for the participant.

3) Payments of tuition, related educational fees, and room and board expenses for the next 12 months of post-secondary education for the participant, the participant's spouse, or the participant's children or dependents.
Six safe harbor events (cont’d)

4) Payments necessary to prevent the eviction of the participant from the participant's principal residence or foreclosure on the mortgage on that residence

5) Payments for burial or funeral expenses for the employee's deceased parent, spouse, child or dependent

6) Expenses for the repair of damage to the employee's principal residence that would qualify as a casualty deduction
Required documentation

- New informal IRS guidance – April 2017
- Even if you use a third party administrator, it’s your responsibility
- IRS emphasized must keep proper documentation
- NOT okay to ask participants to keep documentation
IRS wants you to have:

1) Documentation of the hardship request, review and approval

2) Financial information and documentation that substantiates the employee’s immediate and heavy financial need

3) Documentation to support that the hardship distribution was properly made in accordance with the applicable plan provisions and the Internal Revenue Code

4) Proof of the actual distribution made and related Forms 1099-R
IRS audit memorandum

- **Substantiation Based on Source Documents:** Obtained before distribution? Substantiate the event?

- **Substantiation Based on a Summary:** Obtained summary before making the hardship distribution? Participant given the required notification and the summary includes all of the information in the attachment to the IRS audit guidelines?
Notification requirements

1) Hardship distribution is taxable and additional taxes could apply

2) Hardship distribution cannot exceed the immediate and heavy financial need

3) Hardship distribution cannot be made from earnings on elective deferrals (or QMACs or QNECs, if any)

4) Participants must agree to retain source documents and make them available at any time, upon request
Notification requirements (cont’d)

- Additional information required

- See IRS document, “Hardship Substantiation Information and Notifications for Summary of Source Documents”
Participant Loans
For every plan loan, need:

1) Evidence of the loan application, review and approval process;

2) An executed plan loan note;

3) If applicable, documentation verifying that the loan proceeds were used to purchase or construct a primary residence;

4) Evidence of loan repayments; and

5) Evidence of collection activities associated with loans in default and the related Forms 1099-R, if applicable.
Residence loans

- Must obtain documentation before the loan is approved
- Cannot allow self-certification
Current industry trends
Current industry trends

- Revenue sharing
- Fee leveling
- Marketing efforts to sell you more stuff, such as HSAs, financial wellness, and participant advice
- Financial wellness
- Advisors and the practice of law
Questions?
Change is in the Air: Form 5500 –
It’s Not Just a “Signature Page”

Jill Pierce, Assurance Senior Manager
Gwen Bryant, Assurance Partner
Form 5500 – It’s Not Just a “Signature Page”
Other Penalties

1. Any individual who willfully violates any provision of Part 1 of Title I of ERISA shall on conviction be fined not more than $100,000 or imprisoned not more than 10 years, or both. See ERISA section 501.

2. A penalty up to $10,000, five (5) years imprisonment, or both, may be imposed for making any false statement or representation of fact, knowing it to be false, or for knowingly concealing or not disclosing any fact required by ERISA. See section 1027, Title 18, U.S. Code, as amended by section 111 of ERISA.
Before you sign...

Review the Form 5500 for accuracy and completeness
Practical Exercise:

Walk through a practical review of Form 5500
Common Errors noted by a Practitioner and the DOL
Form 5500 Modernization Initiative

Proposed changes as published and presented by the DOL, IRS, and PBGC
Purpose of the Form 5500

- Retirement, health and other welfare plans satisfy annual reporting obligations under ERISA and the Internal Revenue Code by filing Form 5500 with any required schedules and attachments.
- In addition to disclosing important information to plan participants and beneficiaries, the Form 5500 is an essential compliance and research tool for the DOL, IRS & PBGC.
- Other federal agencies, Congress, and the private sector also rely on the Form 5500 as an important source of information for accessing employee benefit, tax, and economic trends and policies.

Proposed changes as published and presented by the DOL, IRS, and PBGC.
Developing the proposal was a multi-year, tri-agency effort

Takes into account over 15 reports from the GAO, DOL-OIG, TIGTA, and the ERISA Advisory Council

Agencies considered informal outreach from stakeholders
Targeted for 2019 plan year filings

Proposed changes as published and presented by the DOL, IRS, and PBGC
### Five Major Goals

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Modernize the financial statements and investment information filed about employee benefit plans</td>
</tr>
<tr>
<td>2</td>
<td>• Enhance accessibility and usability of data filed on the forms</td>
</tr>
<tr>
<td>3</td>
<td>• Update reporting requirements for service provider fee and expense information</td>
</tr>
<tr>
<td>4</td>
<td>• Require reporting by all group health plans covered by Title I of ERISA</td>
</tr>
<tr>
<td>5</td>
<td>• Improve compliance through new questions on plan operations and financial management of the plan</td>
</tr>
</tbody>
</table>

*Proposed changes as published and presented by the DOL, IRS, and PBGC*
**Goal #1: Modernize Financial Statements**

Proposal intended to improve transparency and reliability of financial reporting, especially regarding alternative investments, hard-to-value assets, and investments through collective investment vehicles, including direct filing entities (DFEs).

| Changes to the Schedule H balance sheet/income statement for more accurate and detailed reporting on general classes of investments |
| Schedule H, Line 4i (Schedule of Assets) to provide more detailed information on the filer's individual investments |
| Improvements to reporting on pooled investment funds and DFEs |

*Proposed changes as published and presented by the DOL, IRS, and PBGC*
Goal #1 (Continued)

- Better information on plan terminations, mergers, and consolidations
- Better information on investment alternatives in participant-directed 401(k)-type plans
- Schedule G changes for more uniform information on loans, fixed income obligations, and leases in default
- Eliminate Schedule I – Small plans not eligible for 5500-SF invested in hard-to-value/alternative investments would complete more detailed financials on Schedule H

*Proposed changes as published and presented by the DOL, IRS, and PBGC*
Goal #1 (Continued)

- Update Form 5500-SF to help make sure only small plans invested in eligible assets use the simplified Form 5500-SF
- Revise the audit rule for certain small 401(k)-type plans
- New questions on frozen plans and rollovers as business start-ups (ROBs)
- Other questions where the DOL, IRS or PBGC has found compliance issues

Proposed changes as published and presented by the DOL, IRS, and PBGC
Goal #2: Improve Usability of Data

Proposal would convert more elements of the Form 5500 into computer-processable data that can be searched and used for data-mining and analytic purposes.

Proposed changes would also enable private sector data users to develop more individualized tools for employers to evaluate their retirement plans and for employees to manage their retirement savings.

Proposed changes as published and presented by the DOL, IRS, and PBGC.
Goal #2 (Continued)

Central improvement in data mineability is standardizing the Schedule H, Line 4i Schedule of Assets

Schedule of Assets held for Investment and Schedule of Assets Disposed of Within Year

Include investment identifiers, such as CUSIP, CIK, LEI, already used in other industry data collections

Improve reporting of assets held through DFEs and participant-directed accounts

Better identify party-in-interest transactions

Proposal would replace most attachments to Schedules A, G, MB/SB with text fields on schedules

Proposed changes as published and presented by the DOL, IRS, and PBGC
Goal #3: Improve Information on Service Providers and Fees

Harmonizing reporting on Form 5500 Schedule C with the DOL’s now final service provider fee disclosure regulation at 29 CFR 2550.408b-2 would provide a powerful tool for improved evaluation of investment, recordkeeping, and administrative fees and service arrangements.

Require reporting of indirect compensation for service providers and types of compensation described in 408b-2 regulation.

Reporting thresholds correspond to 408b-2:

- Service providers who get $1000+ in indirect compensation
- Other service providers who get $5000+ in direct compensation only
- Eliminate “eligible indirect compensation”

Proposed changes as published and presented by the DOL, IRS, and PBGC.
Goal #3 (Continued)

- Small pension plans not eligible to file the Form 5500-SF would complete Schedule C.
- Large welfare plans that file Schedule C would follow 408b-2 definitions.
- DC pension plans would attach 404a-5 comparison chart to Schedule H/Form 5500-SF.
- Instructions would be clarified on reporting of individual trustee/plan employee expenses including travel reimbursements.

Proposed changes as published and presented by the DOL, IRS, and PBGC.
Goal #4: New Group Health Plan Reporting

Proposal would remedy current failure to collect data about a large sector of the health plan market made up of ERISA group health plans

Goals:
- Establish better compliance awareness amount plans
- Provide critical data for Agency oversight
- Collect information for Congressionally mandated reports
- Satisfy certain reporting requirements under the Affordable Care Act (ACA)

Proposed changes as published and presented by the DOL, IRS, and PBGC
Goal #5: Improve Compliance

The proposed revisions are intended to enhance reporting on compliance to improve plan operations, protect participants and beneficiaries and their benefits, and to educate and provide annual discipline for plan fiduciaries.

- Fiduciaries need to evaluate plan compliance under ERISA and the IRC as part of completing the Form 5500.
- Form will provide the Agencies with improved tools to focus oversight and enforcement resources.
- New questions regarding plan operations, service provider relationships, financial management of plans.
- New questions to Schedule R asking for information specific to DC pension plan participation and enrollment, contribution and matches.
- New questions on investment alternatives and qualified default investment alternatives (QDIAs) in participant directed defined contributions plans.

Proposed changes as published and presented by the DOL, IRS, and PBGC.
Insurance (Schedule A)

New questions ask for additional information on fees and commissions, premium payment delinquencies, and insurer identifying information (NAIC Company Code, HPID)

Instructions clarify rule on counting covered lives under an insurance contract

New questions and breakouts on variable annuities

Proposed changes as published and presented by the DOL, IRS, and PBGC
ESOPs (Schedule E)

Proposal would reinstate Schedule E to improve information on employee stock ownership plans (ESOPs). Before 2009, Schedule E was part of Form 5500

Proposed new Schedule E would include some of the question on the pre-2009 Schedule E, revisions to other questions, and additional new questions, as well as include the ESOP-specific questions currently on the Schedule R

Proposed changes as published and presented by the DOL, IRS, and PBGC
Actuarial Information (Schedules MB and SB)

Expand data elements for multiemployer (MB) and single-employer (SB) defined benefit plans

Report more information in data mineable format

More refined projections of plans’ financial positions

More refined projections of future coverage and benefit adequacy for plan participants and beneficiaries

Target plans with likely compliance issues and assist auditors in validating a plan actuary’s calculations

*Proposed changes as published and presented by the DOL, IRS, and PBGC*
Potential Impact of Form 5500 Changes

- Form 5500 returns more easily “mineable”
- “Improved” transparency
- More questions + schedules = time (and $)
Exposure Draft.... More Changes

• Proposed Statement on Auditing Standards (SAS) - EBP
• Auditing Standards Board (ASB) - task force (DOL participating)
• Potential reporting models – similarities to GAGAS
  • Reporting on internal controls over financial statements,
  • Compliance with laws and regulations
  • Findings
Exposure Draft

• SAS AU-C 705 expected April 2017
• Comment period – likely will be 100 days
• Background, potential changes
Plan Audit Report

For a “limited scope” audit, attach certification(s) that meet new requirements

Name of audit engagement partner

Reasons for omitted IQPA report

Identify state in which the opinion is issued

Information on communications with or from the IQPA and disclosures

Information about the peer review of the IQPA

*Proposed changes as published and presented by the DOL, IRS, and PBGC*
IRS Corner

Electronic Filing Mandate

IRS-Only Questions

Form 5500-SUP

Possible new schedule for IRS only questions

Add Form 5500-EZ and Form 5558

E-signature option for actuary signature and trustee signature

Proposed changes as published and presented by the DOL, IRS, and PBGC
Key Take-Aways

- Review Form 5500 carefully before signing
- Understand the key (expected) changes to the Form 5500 and its impact
- Comment on exposure draft of SAS
Questions / Contact Information

Jill Pierce
(479) 521-9191
jpierce@hogantaylor.com
www.hogantaylor.com

Gwen Bryant
(479) 521-9191
gbryant@hogantaylor.com
www.hogantaylor.com
Cyber Security Issues for Employee Benefits

Cody Griffin, CPA, CITP, CISA
Partner, HoganTaylor LLP

Gwen Bryant, CPA
Partner, HoganTaylor LLP
CODY GRIFFIN, CPA, CITP, CISA
RISK ASSURANCE PARTNER
Cody began his career in the risk assurance and advisory practice of PricewaterhouseCoopers and joined HoganTaylor in 2013. He is a CPA, CITP and CISA with over 14 years of experience in both public and private industry. Cody’s industry experience includes information technology, telecommunications, retail, financial institutions, energy, higher education and transportation. His areas of practice include Sarbanes-Oxley (SOX) Section 404, IT audit, business process reviews, service organization control audits (SSAE 16), Fraud reviews, agreed upon procedures, internal audit assurance services and compliance audits. Cody leads firm in providing "Attack & Penetration" services, which assists HoganTaylor clients in identifying vulnerabilities in their IT infrastructure. Cody graduated from Oklahoma State University with a B.S. in Accounting and received his M.B.A. from Texas Tech University in Management Information Systems.
Session Overview

- IT Security Risks
  - Network Attacks
    - Recent Attacks / Data Breaches
    - Cost of a Data Breach
  - Social Engineering
  - BYOD
  - Cloud / Third-party Service Providers
- Cybersecurity and Employee Benefit Plans
  - Choosing and Monitoring Service Providers
  - Protecting Data
  - Staying Up-to-Date on Industry Standards
  - Cyber Liability Insurance
Network Attacks

Top Network Attacks in Q1 2017

Top 2017 Threats to Cybersecurity

- Hardware
- Ransomware
- Software Vulnerabilities
- Cloud Services
- Wearables
- Connected Cars
- Warehouses of Stolen Data
- Hactivism
Data Breaches

DATA RECORDS COMPROMISED IN 2016

1,378,509,261

3,776,738 records lost or stolen every day
157,364 records every hour
2,623 records every minute
44 records every second
Data Breaches

Gemalto
Data Breaches

Data Breaches by Industry

- Healthcare: 493 incidents (28%)
- Government: 269 incidents (15%)
- Other: 229 incidents (13%)
- Retail: 215 incidents (12%)
- Financial: 214 incidents (12%)
- Technology: 189 incidents (11%)
- Education: 157 incidents (9%)

Gemalto
Data Breaches

NUMBER OF RECORDS BREACHED BY INDUSTRY IN 2016

- **EDUCATION**: 4,370,002 RECORDS (<1%)
- **HOSPITALITY**: 9,569,173 RECORDS (<1%)
- **FINANCIAL**: 13,323,589 RECORDS (19%)
- **RETAIL**: 32,551,173 RECORDS (21%)
- **HEALTHCARE**: 35,279,635 RECORDS (23%)
- **TECHNOLOGY**: 391,653,136 RECORDS (28%)
- **GOVERNMENT**: 391,687,371 RECORDS (28%)
- **OTHER**: 500,075,182 RECORDS (36%)

**TOTAL RECORDS**: 1,378,509,261

Source: BREACHEXINDEX.COM
January 2016 to December 2016
# Data Breaches

## Number of Breach Incidents by Industry Over Time

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>345</td>
<td>448</td>
<td>445</td>
<td>493</td>
</tr>
<tr>
<td>Government</td>
<td>194</td>
<td>290</td>
<td>297</td>
<td>269</td>
</tr>
<tr>
<td>Other Industries</td>
<td>262</td>
<td>275</td>
<td>321</td>
<td>229</td>
</tr>
<tr>
<td>Retail</td>
<td>98</td>
<td>195</td>
<td>239</td>
<td>215</td>
</tr>
<tr>
<td>Financial Services</td>
<td>165</td>
<td>212</td>
<td>276</td>
<td>214</td>
</tr>
<tr>
<td>Technology</td>
<td>112</td>
<td>139</td>
<td>122</td>
<td>189</td>
</tr>
<tr>
<td>Education</td>
<td>35</td>
<td>174</td>
<td>165</td>
<td>157</td>
</tr>
<tr>
<td>Hospitality</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>26</td>
</tr>
</tbody>
</table>

Source: BREACHLEVELINDEX.COM
Data Breaches

World's Biggest Data Breaches
Selected issues greater than 10,000 records
Updated 20th Apr 2013

IT'S A JUNGLE OUT THERE
THE 2017 EMPLOYEE BENEFIT PLAN UPDATE
Cost of a Data Breach

Figure 5. Per capita cost by industry classification

*Historical data are not available for all years

Measured in USD

IBM / Ponemon Institute 2017
Cost of a Data Breach

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach

- Malicious or criminal attack: 47%
- System glitch: 25%
- Human error: 28%
### Cost of a Data Breach

**Figure 9. Impact of 20 factors on the per capita cost of data breach**

Measured in US$

<table>
<thead>
<tr>
<th>Factor</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident response team</td>
<td>19.3</td>
</tr>
<tr>
<td>Extensive use of encryption</td>
<td>16.1</td>
</tr>
<tr>
<td>Employee training</td>
<td>12.5</td>
</tr>
<tr>
<td>BCM involvement</td>
<td>10.9</td>
</tr>
<tr>
<td>Participation in threat sharing</td>
<td>8.0</td>
</tr>
<tr>
<td>Use of security analytics</td>
<td>6.8</td>
</tr>
<tr>
<td>Extensive use of DLP</td>
<td>6.2</td>
</tr>
<tr>
<td>Data classification schema</td>
<td>5.7</td>
</tr>
<tr>
<td>Insurance protection</td>
<td>5.4</td>
</tr>
<tr>
<td>CISO appointed</td>
<td>5.2</td>
</tr>
<tr>
<td>Board-level involvement</td>
<td>5.1</td>
</tr>
<tr>
<td>CPO appointed</td>
<td>2.9</td>
</tr>
<tr>
<td>Provision of ID protection</td>
<td>(2.0)</td>
</tr>
<tr>
<td>Consultants engaged</td>
<td>(2.7)</td>
</tr>
<tr>
<td>Rush to notify</td>
<td>(5.5)</td>
</tr>
<tr>
<td>Lost or stolen devices</td>
<td>(7.6)</td>
</tr>
<tr>
<td>Extensive use of mobile platforms</td>
<td>(8.8)</td>
</tr>
<tr>
<td>Compliance failures</td>
<td>(11.2)</td>
</tr>
<tr>
<td>Extensive cloud migration</td>
<td>(14.3)</td>
</tr>
<tr>
<td>Third party involvement</td>
<td>(16.9)</td>
</tr>
</tbody>
</table>

---

IBM / Ponemon Institute 2016
## Cost of a Data Breach

### Table 1

**Data loss prevention controls and activities**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint security solutions</td>
<td>30%</td>
<td>41%</td>
<td>42%</td>
<td>40%</td>
<td>55%</td>
<td>50%</td>
<td>48%</td>
</tr>
<tr>
<td>Training and awareness programs</td>
<td>67%</td>
<td>63%</td>
<td>53%</td>
<td>51%</td>
<td>51%</td>
<td>50%</td>
<td>52%</td>
</tr>
<tr>
<td>Expanded use of encryption</td>
<td>58%</td>
<td>61%</td>
<td>52%</td>
<td>52%</td>
<td>50%</td>
<td>52%</td>
<td>49%</td>
</tr>
<tr>
<td>Additional manual procedures and controls</td>
<td>58%</td>
<td>54%</td>
<td>49%</td>
<td>46%</td>
<td>43%</td>
<td>40%</td>
<td>41%</td>
</tr>
<tr>
<td>Data loss prevention (DLP) solutions</td>
<td>42%</td>
<td>43%</td>
<td>45%</td>
<td>49%</td>
<td>35%</td>
<td>39%</td>
<td>38%</td>
</tr>
<tr>
<td>Identity and access management solutions</td>
<td>49%</td>
<td>52%</td>
<td>47%</td>
<td>43%</td>
<td>39%</td>
<td>40%</td>
<td>41%</td>
</tr>
<tr>
<td>Security intelligence solutions</td>
<td>22%</td>
<td>21%</td>
<td>26%</td>
<td>28%</td>
<td>34%</td>
<td>37%</td>
<td>39%</td>
</tr>
<tr>
<td>Other system control practices</td>
<td>40%</td>
<td>43%</td>
<td>38%</td>
<td>34%</td>
<td>33%</td>
<td>32%</td>
<td>30%</td>
</tr>
<tr>
<td>Strengthening of perimeter controls</td>
<td>20%</td>
<td>22%</td>
<td>25%</td>
<td>23%</td>
<td>21%</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>Security certification or audit</td>
<td>33%</td>
<td>29%</td>
<td>19%</td>
<td>19%</td>
<td>20%</td>
<td>19%</td>
<td>21%</td>
</tr>
</tbody>
</table>

*Please note that a company may be implementing more than one preventive measure.*

IBM / Ponemon Institute 2016
Social Engineering

Social Engineering Attack
Because There Is No
Guaranty to Human
Instinctivity

Phishing

Social Engineering

IT'S A JUNGLE OUT THERE
THE 2017 EMPLOYEE BENEFIT PLAN UPDATE
BYOD

BRING YOUR OWN DEVICE
BYOD

Growing BYOD Trends

2013:
- SMBs supporting BYOD will increase by 14%
  - 2012: 59%
  - 2013: 73%

2014:
- Number of connected devices: 3.3/employee
- Gartner predicts 90% of companies will allow BYOD

Employee tablet use will see a year-to-year increase of 50%
- 1.2 billion smartphones will enter the market in the next 5 years

HoganTaylor

IT'S A JUNGLE OUT THERE
THE 2017 EMPLOYEE BENEFIT PLAN UPDATE
BYOD (Bring Your Own Device)
Guidance for private and public sector organisations considering a BYOD approach

Limit the information shared by devices
Staff are used to sharing their information with other people and in the cloud. Considered backup of device data to cloud-based accounts can lead to business data being shared.

Understand the legal issues
The legal responsibility for protecting sensitive personal information is with the data controller, not the device owner.

Create effective BYOD policy
Ensure that personally-owned devices are only able to access business data that you are willing to share with authorised staff.

Anticipate increased device support
Your services may need to be adjusted to different types of device. Make sure you have the IT support capability and structure to manage a growing range of devices.

Encourage staff agreement
Communicate your BYOD policy through staff training so they understand their responsibilities when using personally-owned devices for work purposes.

Consider alternative ownership models
Remote devices may not always be secured. Consider using policies to ensure that personally-owned devices are password protected and controlled by your organisation.

Consider using technical controls
Container applications and mobile threat management can help you monitor and manage personally-owned devices, but they may impact usability of the device.

Plan for security incidents
When there is a security breach, consider whether the maker of the device is responsible, or the device owner, or the business. Each individual case may need different consideration.

IT'S A JUNGLE OUT THERE
THE 2017 EMPLOYEE BENEFIT PLAN UPDATE
HoganTaylor
Cloud / Third-party Service Providers

PROTECTING YOUR DATA WHEREVER IT GOES
The top 4 places your files are at risk

Only 2% of vendors have security certifications.

Only 1 OUT OF 5 third-party vendor contracts contain security provisions.

5.6 MILLION Credit cards stolen during the Home Depot breach of 2014.

The cause? Hackers were able to access the database by stealing the credentials of a third-party vendor.

88% of companies have experienced some sort of data loss due to emails.

Each email is copied by an average of six times, greatly increasing the risk of exposure.

113 cell phones are lost or stolen every minute in the U.S.

36% of mobile apps lack adequate security.

15% of enterprises require a password for mobile devices.

Seclore, an award-winning provider of information-centric security solutions, helps organizations achieve their security, privacy and compliance objectives through its innovative Information Rights Management software. Learn more at www.seclore.com


IT'S A JUNGLE OUT THERE
THE 2017 EMPLOYEE BENEFIT PLAN UPDATE

Hogan Taylor
Cyber Security and Employee Benefit Plans

- The largest insurance companies in America struggle to keep sensitive data safe
- What about my plan?
Cyber Security and Employee Benefit Plans

• DOL has begun raising concerns
• Responsibility for cyber security resides with the Plan administrator
Cyber Security and Employee Benefit Plans

- Choose and monitor service providers
- Implement procedures to protect data
- Stay up to date on industry best practices
- Explore Cyber Liability Insurance
## Choosing new service providers and continuous monitoring

### Questions to ask your service provider

<table>
<thead>
<tr>
<th>Question</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>How do you manage electronic data?</td>
<td>- both in flight (being manipulated or moved) and at rest (sitting in storage)</td>
</tr>
<tr>
<td>How do you secure the physical hardware storing the data?</td>
<td>- including the facility, printers and portable hardware (laptops, tablets, smartphones)</td>
</tr>
<tr>
<td>How do you manage your employees that interact with the data?</td>
<td>- the “Human Factor”</td>
</tr>
<tr>
<td>How do you monitor for suspicious activity?</td>
<td></td>
</tr>
<tr>
<td>How do you react to potential security breaches?</td>
<td></td>
</tr>
</tbody>
</table>

Note: Most of this information is covered in your service provider’s SOC1 report, which should be reviewed annually.
What can I do as Plan Sponsor?
**What can I do as Plan Sponsor?**

<table>
<thead>
<tr>
<th>Implement procedures to protect data</th>
<th>Use caution when handling participant information (social security numbers, dates of birth, email addresses, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Limit access to participant’s online personally identifiable information to few individuals</td>
</tr>
<tr>
<td></td>
<td>Know your company’s cyber security policy</td>
</tr>
<tr>
<td></td>
<td>Appropriately destroy hard copies of documents</td>
</tr>
</tbody>
</table>
What can I do as Plan Sponsor?

<table>
<thead>
<tr>
<th>Stay up to date on industry best practices</th>
<th>Explore current legal and regulatory concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Understand the applicable state laws should there be a data breach</td>
</tr>
<tr>
<td></td>
<td>Attend seminars in person and on the web</td>
</tr>
<tr>
<td></td>
<td>Regularly review updates on the IRS and DOL websites</td>
</tr>
<tr>
<td></td>
<td>Consider engaging an attorney with ERISA expertise</td>
</tr>
</tbody>
</table>
## What can I do as Plan Sponsor?

<table>
<thead>
<tr>
<th>Explore cyber liability insurance</th>
<th>Understand what your general business insurance policy does and does not cover</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cyber liability insurance helps mitigate the administrative, technological and legal costs of a data breach</td>
</tr>
<tr>
<td></td>
<td>Can help provide the Plan with experienced attorneys, forensic experts and public relations professionals</td>
</tr>
</tbody>
</table>
Questions / Contact Information

Cody Griffin
(501) 227-4343
cgriffin@hogantaylor.com
www.hogantaylor.com
Thank You for Joining Us Today