

Snell & Wilmer

Yes, Virginia, there is a Cyber Clause!

**Data Privacy and Security
for Employee Benefit Plans**


*Western Pension & Benefits Council
Phoenix Chapter
December 10, 2015*

Patrick X. Fowler • Snell & Wilmer L.L.P.
One Arizona Center • Phoenix, AZ 85023
602.382.6213 • pfowler@swlaw.com

© 2015 Snell & Wilmer

Presenter

Patrick X. Fowler
Snell & Wilmer LLP
Chair of the Privacy, Data Protection and Cybersecurity Practice



Pat's practice concentrates on defending companies facing high-stakes business, technology and product liability claims.

Pat helps clients dealing with internet/e-commerce disputes, data privacy and cybersecurity concerns, and e-discovery issues. He helps to develop information governance policies and procedures, draft contracts involving privacy, data protection and cybersecurity terms, prepare data breach response plans, create and update privacy policies, and navigate the complex regulatory field involving cybersecurity and privacy.

Among other organizations, Pat is an executive committee member of the State Bar of Arizona's Standing Committee on Technology and the e-Commerce/Internet Section. He is also a member of the International Association of Privacy Professionals.

Education:
University of Kansas School of Law (J.D. 1988; B.A. Molecular Biology, 1983)

Professional Recognition

- *The Best Lawyers in America*® - (2016)
- *Southwest Super Lawyers*®

2 © 2015 Snell & Wilmer

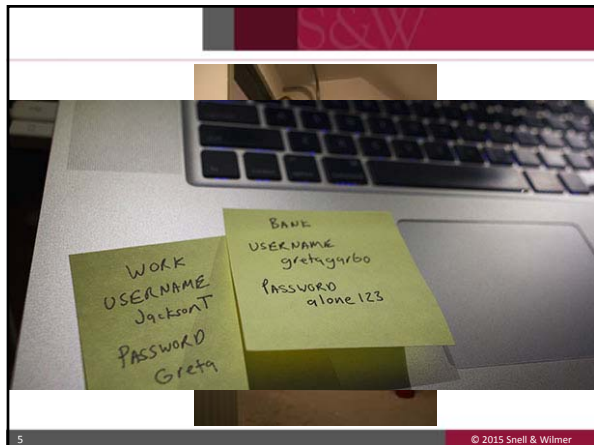
Data Security

It's Not a Matter of If, But When...

- **No one** is immune from the risk of a data breach
 - Governments, non-profits, academia, businesses of all sizes
- Even the best funded, most well-prepared organizations experience data breaches
 - Why?

3 © 2015 Snell & Wilmer





Recognize the New Normal

- The data you collect and store contains protected personal, health and/or financial information;
- You are subject to multiple data privacy and security laws and/or regulations;
- You will likely experience a data loss incident or breach at some point in time (if you haven't already);
- A data breach can cause significant financial and brand reputation damage; and
- Ignoring the risk won't make it go away.

Source: 2015 Data Protection and Breach Readiness Guide, Online Trust Alliance (February 13, 2015)

The slide number "6" is in the bottom left corner, and the copyright "© 2015 Snell & Wilmer" is in the bottom right corner.

Cyber Threat Environment

- 70% of cyber-attacks go undetected
- Average time to detect a cyber-attack: **205 days**
- New malware signatures released *each day*: **> 70,000!**



10 © 2015 Snell & Wilmer

Cyber Threat Environment

<ul style="list-style-type: none"> • Annual global corporate losses to cyber crime and data breaches: 	<ul style="list-style-type: none"> • Annual global corporate spending on cybersecurity solutions:
2014: \$375 - \$575 billion	2015: \$ 75 billion
2019: \$2.1 trillion	2020: \$170 billion



11 © 2015 Snell & Wilmer

Data Breach Trends

Data Breach Causes and Consequences

- Cyber-attacks are only one cause of data breach events.
 - Human error and system failure cause also cause data breaches.
- Regardless of the cause, **data breaches are expensive.**
 - In the US, the **average** total cost per reported data breach is **~\$6.5 million** (\$217 per record x 30,000 records per reported breach)
 - **\$7.7 million** per record if **financial records** (\$259/record)
 - **\$11.9 million** per record if **medical records** (\$398/record)
 - 1/3 of costs go to detection, notification, remediation, recovery
 - 2/3 of costs are for lost customers/business due to data breach

12 © 2015 Snell & Wilmer

2015 Data Breach Statistics

- As of December 8, 2015*:
 - 732 separate data breach events reported
 - 176 million records exposed
- Biggest reported breaches in 2015 (U.S. companies):
 - **Anthem, Inc.:** 79 million records
 - U.S. Ofc. of Personnel Management: >25 million records
 - T-Mobile/Experian: 15 million records
 - **Premera Blue Cross:** 11 million records
 - **Excelsus Blue Cross Blue Shield:** 10 million records

*Source: Identity Theft Resource Center <http://www.idtheftcenter.org/images/breach/ITRCBreachReport2015.pdf>

13 © 2015 Snell & Wilmer

Other Notable Reported Breaches in 2015

- **UCLA Health Systems**
- **Georgia Dept. Community Health (x2)**
- **Medical Informatics Engineering**
- **A T & T Group Health Plan**
- **Beacon Health System**
- Lastpass
- PNI Digital Media
- Piedmont Advantage Credit Union
- AutoZone
- Sterling Bankcheck
- Firekeepers Casino
- Blue Sky Casino
- Web.com
- Alfa Specialty Insurance
- V-Tech Learning Lodge
- Office of Jeb Bush
- Katy, TX School District
- Penn State University
- Auburn University
- Career Education Corporation
- Metropolitan State University
- Department of Defense
- Internal Revenue Service
- Sally Beauty Holdings
- Ashley Madison
- Utah Food Bank
- Scottrade
- T-Mobile/Experian
- Hilton Hotels
- Dow Jones
- Talk Talk

14 © 2015 Snell & Wilmer

April 2014 FBI Cyber Division Alert

- **Health Care Systems at Risk for Increased Cyber Intrusions for Financial Gain**
 - “Cyber actors will likely increase cyber intrusions against health care systems . . . due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.”
 - “The health care industry is not technically prepared to combat against cyber criminals’ basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APT). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.”

15 © 2015 Snell & Wilmer

April 2014 FBI Cyber Division Alert

- **Health Care Systems at Risk for Increased Cyber Intrusions for Financial Gain**
 - “Cyber criminals are selling the information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number.
 - “EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

16 © 2015 Snell & Wilmer

Anthem Data Breach Info

- February 5, 2015: Anthem announces that its servers were accessed by sophisticated cyber-attackers
 - Beginning on 12/10/14
 - Discovered on 1/29/15 (50 days -- unusually quick)
- Approximately 79 million Anthem customers were affected
 - All insurance lines, not just health

17 © 2015 Snell & Wilmer

Anthem Data Breach Info

- Attackers accessed Anthem’s computers using valid administrator credentials
- Data breach included:
 - Names, addresses, phone numbers
 - Member ID numbers
 - Dates of birth
 - SSN
 - Email addresses
 - Employment info, including income data
- Per Anthem: no health or financial info accessed

18 © 2015 Snell & Wilmer

Advisory Council Report

Benefit Plan Data Breach Examples

- Hacking into the plan’s administrative system after gaining administrative privileges (via a keystroke logging virus);
- Hacking into the broker website, entering ID and password and securing payment which was sent to different account;
- Hacking into database to access 500,000+ participants’ PII, due to failure of the plan to install security updates;
- Email hoax (phishing) directing participants to a look-alike website where they shared PII, including SSNs;

22 © 2015 Snell & Wilmer

Advisory Council Report

Benefit Plan Data Security Risks

- Payroll provider using the same password for all clients when the payroll system was created;
- Returning digital copy machines to leasing company without erasing data on its hard drives;
- Failing to securely dispose of paper records containing confidential information;
- Failing to securely dispose of electronic storage media containing confidential information;
- Sending auditors PII of participants and/or beneficiaries of benefit plans they did not currently audit;

23 © 2015 Snell & Wilmer

Advisory Council Report

Benefit Plan Data Security Risks

- Email hoax (phishing) directing participants to a look-alike website where they shared PII, including SSNs;
- Unencrypted laptops lost or stolen, containing PII;
- Employee downloading confidential information on 450,000 plan participants to a home computer;
- Confidential information (SSNs) on documents mailed (or e-mailed) to the wrong address;
- Printing SSNs or account numbers on mailing labels visible to others.

24 © 2015 Snell & Wilmer

Advisory Council Report

Points of Vulnerability

- Data Management
 - Keeping data that is no longer needed or relevant
 - Lack of controls over back-up copies and who is allowed to access the data
- Technology Management
 - Outdated or poor technology design
 - Inadequate controls over wireless and portable devices
 - Failure to use encryption to keep data secure
 - Failure to apply security patches and updates

25 © 2015 Snell & Wilmer

Advisory Council Report


Points of Vulnerability

- Service Provider (Vendor) Management
 - Assuring that the service provider has appropriate security and privacy systems to protect plan data
- People Issues
 - Hiring the wrong people
 - Inadequate training and management leads to increased risk of social engineering
- Small Business Issues

26 © 2015 Snell & Wilmer

Small and medium businesses (SMBs) are targeted:

- Fewer resources for cybersecurity and data protection;
- Hackers practice new attacks;
- SMBs are portals to bigger fish via access credentials.



27 © 2015 Snell & Wilmer

Advisory Council Report

2011: Recommendations to DOL

The Council recommended that the Dept. of Labor:

- Provide guidance on the obligation of plan fiduciaries to secure and keep private the personal identifiable information (“PII”) of participants and beneficiaries;
- Develop educational materials and outreach efforts for plan sponsors, participants, and beneficiaries to address the issues of privacy and security of PII.

DOL has not yet issued anything in response ...

28 © 2015 Snell & Wilmer

Duty to Protect PII/PHI Under ERISA?

- ERISA does not specifically state whether and how ERISA plans should protect PII/PHI
- HIPAA provides requirements for protecting PHI
- DOL statement – “Understanding Your Fiduciary Responsibilities Under a Group Health Plan”
 - “make sure that the plan complies with ERISA, which includes COBRA, HIPAA and other group health plan provisions in the law
- Discretionary selection of a vendor is a fiduciary function

29 © 2015 Snell & Wilmer

Duty to Protect PII/PHI Under ERISA?

- Who is the fiduciary with delegated authority under the plan document with respect to data privacy and security?
 - Protecting PII and PHI and remediating data breaches
- Is someone acting as a fiduciary with respect to data privacy and security? (ERISA §3(18))
- Plan fiduciaries should evaluate current practices and vendor contracts in light of privacy laws

30 © 2015 Snell & Wilmer

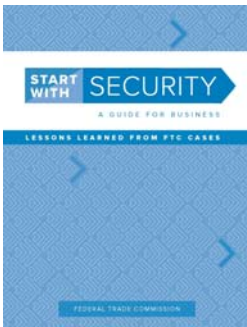
Data Breach Risk Reduction Tips


Going-Forward Steps to Reducing Your Risk of a Data Breach



31 © 2015 Snell & Wilmer

Data Security Tips





32 © 2015 Snell & Wilmer

Data Security Tips


- **Educate your employees on cybersecurity basics**
 - Recognizing phishing and vishing attacks
 - Smart password strategies
 - Remote network access
 - Verifying wire transfer info
- Start at the c-suite.
- Repeat, regularly.



33 © 2015 Snell & Wilmer

Data Security Tips

- **Data minimization** should be in the corporate DNA
 - Don't collect sensitive information you don't need
 - Keep it only as long as you actually need it
 - Only use sensitive information when it is necessary, and for the purpose it was collected



Source: Start With Security—A Guide for Business, Federal Trade Commission (June 2015)

34 © 2015 Snell & Wilmer

Data Security Tips

- **Sensibly Control Access to Data**
 - Restrict access to sensitive data
 - Unless employees have to use personal information as part of their job, there's no need for them to access it
 - Limit administrative access to IT systems
 - Only those employees tasked with making system-wide changes to the computer system should have those rights



Source: Start With Security—A Guide for Business, Federal Trade Commission (June 2015)

35 © 2015 Snell & Wilmer

Data Security Tips

- **Require secure passwords and authentication**
 - Insist on complex and unique passwords
 - Store passwords securely
 - Guard against brute force attacks
 - Limit the number of password attempts before lock-out
 - Protect against authentication bypass
 - Engage in vulnerability testing



You shouldn't share your passwords either.


Be vigilant. Stay safe online.

Source: Start With Security—A Guide for Business, Federal Trade Commission (June 2015)

36 © 2015 Snell & Wilmer

Data Security Tips

- **Store sensitive personal information securely and protect it during transmission**
 - Keep sensitive data secure through its **lifecycle**
 - Implement data encryption
 - Use industry-tested and accepted methods for securing data




Source: Start With Security – A Guide for Business, Federal Trade Commission (June 2015)

37 © 2015 Snell & Wilmer

Data Security Tips

- **Secure paper, physical media and devices, too.**
 - Protect devices that process personal information.
 - Keep data secure while en route. Encrypt!
 - Dispose of sensitive data securely.
 - Selling hard drives on eBay?
 - Placing records in dumpsters?




Source: Start With Security – A Guide for Business, Federal Trade Commission (June 2015)

38 © 2015 Snell & Wilmer

Data Security Tips

- **Plan and prepare for a data loss incident**
 - Create an actionable incident response plan
 - Include an incident response team
 - Practice, evaluate and improve it
 - Develop relationships with relevant law enforcement agencies, experienced outside counsel, PR firm, and investigative and cybersecurity firms
 - **Hope is not a plan.**



Source: Best Practices for Victim Response and Reporting of Cyber Incidents, U.S. Dept. of Justice, Cybersecurity Unit (April 2015)

39 © 2015 Snell & Wilmer

Wrap-up and Questions



40 © 2015 Snell & Wilmer



41 © 2015 Snell & Wilmer

Thank you!

Patrick X. Fowler • Snell & Wilmer L.L.P.
One Arizona Center • Phoenix, AZ 85023
602.382.6213 • pfowler@swlaw.com
@eDataBreachLaw
<http://www.swlaw.com/blog/data-security/>

42 © 2015 Snell & Wilmer
