ERISApedia.com
Get Answers. Win Clients.

Get Your Hands Off My Money! Understanding Identity Theft and Best Practices

Alison J. Cohen, Esq., APA, APR
Adrienne I. Moore, Esq.
Adriana M. Starr, Esq.

FERENCZY
BENEFITS LAW CENTER
ERISA
We are your ERISA solution

1

Your Co-Hosts

- Joanne Pecina

- Maureen Pesek

- Tim McCutcheon

FERENCZY
BENEFITS LAW CENTER
ERISA
We are your ERISA solution

2

2

During the Webinar

- All attendees' lines are muted.
- Question board is available and monitored - look for Q&A icon on webcast toolbar. Please do not use chat to ask questions.
- Slides and a recording of the webinar also available on the /webcasts webpage.
- Please note that you must access the live video portion of the webcast to get CE credit.
- Merely listening on a call-in line or watching a webcast recording is not sufficient for CE credit.

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

3

3

During the Webinar

- Credit is offered for ERPA/ASPPA-ARA/NIPA.
- Those who attend the requisite time in the video portion of the webcast today will receive a certificate by email in a few days (ERPA will take several days longer). - Please check your spam folder.
- Questions about CE credit: support@erisapedia.com.
- After the main presentation please join us for a brief educational session on how to find more information on today's topic on ERISApedia.com.
- At the end you will be presented with a short Google Forms survey. Please let us know how we are doing.

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

4

4

Your Presenters Today

Alison J. Cohen, Esq., APA, APR

Adrienne I. Moore, Esq.

Adriana M. Starr, Esq.

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

ERISApedia.com Get Answers. Win Clients.

5

5

Agenda

- How Identity Theft Can Occur
- Understanding the Liability
- Current Court Cases in the News
- Real-Life Case Studies
- Best Practices to Help Avoid Becoming a Victim
- Final Thoughts

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

ERISApedia.com Get Answers. Win Clients.

6

6

Understanding the Landscape

- 67% of CISOs feel their business is likely to have a data breach or suffer a cyber attack in 2018 (Ponemon, 2018)
- Ransomware attacks are growing at a rate in excess of 350% per year (largest increase is in healthcare) (Cisco, 2017)
- In 2017 the number of malware variants identified increased 88% (Symantec, 2017)
- Global cost of cybercrime exceeded $600B in 2017 (McAfee, 2018)
- 978MM people or companies in 20 countries were victimized in 2017 (2.7MM per day) (Norton – 2018)
- Avg. cost of a U.S. data breach
  - $3.62MM per breach (Ponemon, 2017)
  - $141 per record ($245 in Financial Services)
- 78% of all crimes involve malware, or other web-based attacks (Verizon Data Breach Report, 2018)

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

7

Everyone's 401(k) Account Is at Risk

- Retirement plan accounts have become attractive targets to thieves/hackers
  - Large account balances growing over time
    - Often larger than all other bank and investment accounts owned by individuals
    - Per Fidelity Investments, the average 401(k) account balance is > $104,000
  - Participants are often encouraged to not look at their accounts frequently to mitigate day trading or emotional investing
    - Means that accounts are often unmonitored

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

ERISApedia.com Get Answers. Win Clients.

8

8

Everyone's 401(k) Account Is at Risk

- Institutions
  - Smaller institutions may have poor controls/training
  - Some large recordkeepers may have no direct personal relationship with participants – which may make fraud easier to perpetrate

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

ERISApedia.com Get Answers. Win Clients.

9

9

How Identity Theft Can Occur

- Social Engineering is the most common form of 401(k) account fraud
- Social Engineering is psychological manipulation designed to cause people to disclose personal and confidential information
  - Sob story/pull at your heart-strings
  - Call you by name/pretend familiarity
  - A compelling explanation
  - "Sweet talking"
- Usually just one step in a complex scheme

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

10

10

Social Engineering Prevention

- Humans are the weak link in this process
- Have stringent controls regarding the requirements for account access and the disclosure of sensitive information
  - Have a written policy in place, and ENFORCE it
- Educate all employees on the types of attacks being employed
- Don't confuse excellent customer service with handing criminals the keys to the kingdom

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

11

11

Berman v. Estee Lauder

- $12,000 withdrawn 9/29/16
- $37,000 withdrawn 10/7/16
- $50,000 withdrawn 10/18/16
- Berman gets first notice on 10/10/16 and immediately contacts Hewitt Customer Svc.
- Between 10/24/16 – 1/2/17, Berman makes 23 calls to customer service and gets nowhere

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

12

12

Berman v. Estee Lauder (cont.)

- 10/25/16 Berman reports theft to SFPD and FBI
  - She's also smart enough to place a fraud alert with Equifax
- 11/7/16 – Custodian requests Berman completes an Affidavit of Forgery, then crickets…..
- Finally, Berman has enough and files her lawsuit on 10/9/19
- May 2020 – undisclosed settlement has been reached

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

13

13

Bartnett v. Abbott Labs

- 12/29/18 – Request for password reset from unknown phone number.
  - Thief had DOB and last 4 of SSN.
  - Had code sent to email, but Barnett never received. Thief used info to change direct deposit information.
- 12/31/18 – Service Rep disclosed home address to thief.
- 1/01/19 – RK mails confirmation notification despite Bartnett's election to receive email notices.
- 1/08/19 – Second request for password change. Code emailed again. $245,000 request approved.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

14

14

Bartnett v. Abbott Labs (cont.)

- 1/09/19 – Recordkeeper mails confirmation again, not email, and discloses address to thief.
- 1/14/19 – $245,000 transferred to SunTrust account. Bartnett receives notification of withdrawal request.
- 1/15/19 – Barnett immediately notifies Abbott and Police.
- Recovered $59,500 from SunTrust and $48,900 in taxes withheld from the withdrawal.
- 12/2019 – Barnett rejects Abbott's settlement offer of 10%.
- 04/03/20 – Bartnett files lawsuit. (Is anyone surprised?)

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

15

15

Leventhal v. MandMarblestone

- Dec. 2015 – A participant (and Plan trustee) requests $15,000 distribution via email.
- A fraudster gains access to Leventhal's system.
  - TPA claims that an employee was allowed to work remotely and use her personal email address for official duties, which gave the fraudster access to Leventhal's system.
- Fraudster, posing as an office administrator of Leventhal, submits falsified distribution requests via email totaling over $400,000.
  - The communications appeared to originate from Leventhal's office email.
  - Money was sent to an account not previously associated with the participant/trustee.
- Who is the fiduciary? Leventhal is named fiduciary in the Plan. Both TPA and the Custodian deny being fiduciaries.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

16

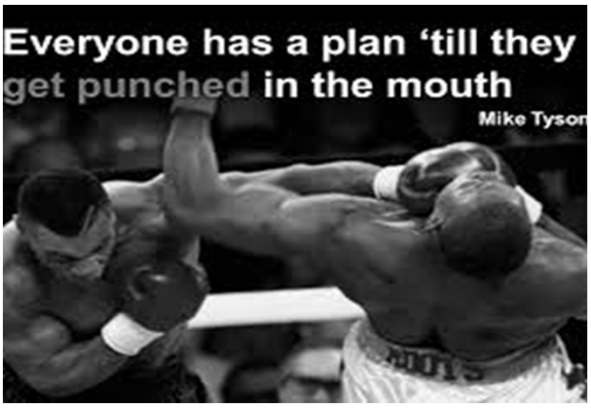
16

Leventhal (cont.)

- Leventhal claims TPA and Custodian are (1) fiduciaries, and (2) jointly and severally liable for any breach.
  - ERISA 405(a) – Fiduciaries may be liable for the breaches of co-fiduciaries.
  - Judge preliminarily determines that breaching co-fiduciaries are jointly and severally liable.
- TPA seeks contribution and indemnity from Leventhal via counterclaim (i.e., if Leventhal also breached its duties, it should be proportionately liable for any losses).
  - Judge allows claim to go forward, based on general trust law, as there is no contrary precedent in the 3d Cir. and it is not explicitly prohibited by ERISA.
- Judge does not decide whether TPA and Custodian are fiduciaries.
  - Possible fiduciary status was sufficiently plead for claim to go forward. If Custodian is a fiduciary, its agreement disclaiming liability violates ERISA.

FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

Real Life Case Studies



FERENCZY BENEFITS LAW CENTER ERISA We are your ERISA solution

Case Study #1

- TPA's employee opens a phishing email.
- TPA immediately notifies IT Company that employee clicked the email. IT does not detect any threats.
- The following week TPA is notified that the employee's email is sending out phishing emails.
- IT immediately disables account and confirms that an outside party accessed the account.
  - New security protocols put in place
- TPA sends out notification of the breach to its current clients.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

19

19

Case Study #1 (cont.)

- TPA maintains insurance that covers the personal data breach and files a claim.
- IT completes a forensic review of the email box for personal data. The review returns thousands of emails that contain personal data.
  - User never cleaned out email box, so emails go back years
- TPA must review the 2,000 emails and prepare a list of individuals affected by the breach.
- Insurance requires TPA to use approved provider for credit monitoring and notification.
  - Cost of mailing is about $1 per head. Then, add in cost of monitoring service at $25-$30 per head. Additional costs if anyone is violated.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

20

20

Case Study #1 (cont.)

- TPA does not have addresses for all of the affected individuals.
  - TPA provides services to other TPAs, so many affected clients aren't even theirs.
- Notification of the breach, including free credit monitoring, is sent to the affected individuals in eight states.
- Each state has different data breach laws.
  - The approved provider does not provide state notification support, so it's now the client's responsibility to figure this out.
- Calls start coming in to TPA during the first few weeks, then die down.
  - Less than 10% of the notified participants request the monitoring.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

21

21

Case Study #2

- Plan Sponsor submits a legitimate request for distribution to the TPA.
- TPA's employee opens a phishing email.
- Fraudster gains access to the employee's email account.
- Fraudster creates false email addresses that appear to be genuine and uses them to communicate with both TPA and Plan Sponsor.
  - Changes distribution instructions from check to wire.
  - Obtains bank account information for the participant from Plan Sponsor.
- TPA wires distribution to the bank account provided by the fraudster.
- Money never arrives at participant's account.
- Plan Sponsor reaches out to TPA via a different contact.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

22

22

Cast Study #2 (cont.)

- TPA contacts its IT professional, who audits system and determines that no breach occurred.
  - Plan Sponsor believes TPA is liable and demands reimbursement.
  - TPA denies reimbursement based on IT professional's assertion.
- TPA maintains cybersecurity insurance for such breaches. Because a demand was made, TPA still files a claim.
- Insurer advises TPA to hire an outside IT firm to perform an independent audit. (Great advice!)
- Independent audit identifies:
  - The original phishing email used to access the TPA employee's account.
  - A forwarding rule implanted by the fraudster gave him access to emails for several weeks. Approximately 450 emails were forwarded to the fraudster under the rule.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

23

23

Case Study #2 (cont.)

- TPA agrees to settlement with the Plan Sponsor and reimburses the money to the participant (ultimately, funds were covered by insurance).
- TPA, with assistance of the outside IT firm, implements new security protocols.
  - Passwords changed and fraudster's access cut off.
  - Email forwarding rule disabled.
  - System updates and Multi-Factor Authentication enabled.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

24

24

Case Study #2 (cont.)

- TPA audits emails that had been forwarded for personal information.
  - Personal information was potentially exposed for five individuals.
  - Data includes names, DOB, address, SSN.
- TPA must notify all affected individuals and state agencies, as applicable.
  - Five different state laws at issue. We advised TPA on reporting requirements.
  - Insurer provided credit monitoring services to the affected individuals.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

25

25

Case Study #3

- "Participant" calls TPA asking how he can get an in-service distribution.
- TPA sends "Participant" back to Plan Sponsor for a distribution form.
- Distribution form arrives at TPA's office requesting in-service withdrawal of $450,000.
  - Signed by HR Director as Plan Administrator.
  - Notarized signature of spouse.
- "Participant" calls TPA's office after form received to confirm it is being processed.
- TPA processes form and, three days later, the actual Participant calls to ask where his money went.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

26

26

Case Study #3 (cont.)

- What did the TPA do right?
- What did the TPA do wrong?
- What could the TPA have done differently?
- What other questions do you have?

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

27

27

Case Study #3 (cont.)

- TPA takes the extra steps and calls the RK/Custodian requesting to put a stop on the transfer.
- TPA calls the receiving bank trying to get the funds returned.
- "Participant" calls back trying to find out why money isn't available for immediate withdrawal.
- Only the federal and state withholding amounts remain to be returned to the Participant's account.
- FBI is contacted and plants an agent in the TPA office, taps phones, etc., in case "Participant" calls back.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

28

28

Understanding the Liability

- When PII is stolen, the responsibility lies with both the service provider that disclosed the information and the plan fiduciaries.
  - Were the existing data protection procedures reasonable?
    - Were they applied and enforced?
  - Was the risk reasonably considered?
  - Was there an opportunity to prevent the risk or recover the data?
  - Did the responsible fiduciary satisfy their duties in hiring and monitoring the service provider?
    - In other words, did they even ask about cybersecurity?

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

29

29

Liability Issues

- When plan assets are stolen, victimized participants will look to the plan administrator, recordkeeper, and/or plan sponsor to make them whole
- But is the participant entitled to restitution? Maybe…
- Not much case law on the issue
  - Two primary cases to illustrate the risks
  - And the bottom line - you better have a reasonable process in place…

30

30

Reasonable Procedures

- What are "reasonable procedures" to safeguard plan assets?
  - TPAs, recordkeepers, custodians, plan sponsors, etc., should be asking:
    - Does each entity have a documented cyber- and data-security policy in place?
      - How often are the procedures reviewed, tested, and revised?
      - Are employees trained on the risks?
    - How is PII transmitted and how is it stored?
    - What procedures are in place to protect PII from improper disclosure?
    - What is the policy on breach notification?
    - What password policies exist for access to sensitive data or plan or participant accounts?
      - Is Multi-Factor Authentication available?

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

31

31

Best Practices

- Client Communications
  - Requiring use of a secure portal
  - Email warning footer regarding failure to use secure portal
  - Article/newsletter to clients regarding protection of data
    - Even just forwarding articles written by others can be helpful

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

32

32

Best Practices (cont.)

- Client Procedures
  - How do they communicate payroll information?
  - How many people have access to confidential client information?
  - Do they have internal procedures to double-check requests?
    - Basic due diligence standard recommendations
    - Creation of verification checklist
    - Have them confirm ERISA bond covers breach

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

33

33

Best Practices (cont.)

- TPA Practices
  - Best Practice Considerations:
    - Implementation of internal basic checklist for reviewing withdrawal/loan applications
    - Use of a threshold dollar amount for special attention
    - Possible temporary freeze for withdrawals/loans on accounts after address changes
      - How does this play into SOX requirements?
    - Implementation of secondary PIN
    - Service agreement provisions to outline procedures and limit liability for actions outside procedures by participant or plan sponsor

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

34

34

Participant Best Practices

- Change to all electronic statements and billing from paper copies
- Remove identifying information from social media
- Change passwords to high security/random
  - Use services like Dashline, Norton, etc.
- Freeze credit
- Utilize alerts on credit cards, bank accounts, etc.

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

35

35

Questions?

FERENCZY BENEFITS LAW CENTER ERISA We are your solution

36

36

FERENCZY
BENEFITS LAW CENTER
ERISA
We are your solution

Contact Us!

ERISApedia.com
Get Answers. Win Clients.

Alison J. Cohen, Esq., APR, APA
678.399.6604 (v)
acohen@ferenczylaw.com

Adriana M. Starr, Esq.
678.399.6610 (V)
404.320.1105 (F)
astarr@ferenczylaw.com

Adrienne I. Moore, Esq.
678.399.6606 (V)
404.320.1105 (F)
amoore@ferenczylaw.com

37

CE Credit

- Credit is offered for ERPA/ASPPA-ARA/NIPA
- Those that attended the requisite time in the live video portion of the webcast today will receive a certificate by email in a few days (ERPA will take longer).
- Please check spam folder.
- Any questions? Email: support@erisapedia.com.
- After the webcast you will be presented with a short Google Forms survey. Please let us know how we are doing.

FERENCZY
BENEFITS LAW CENTER
ERISA
We are your solution

38