




EMPLOYEE RETIREMENT INCOME SECURITY ACT (ERISA)


1




Caleb J. Brus
Attorney

 caleb.brus@brownwinick.com

 515-558-8867

 <https://www.brownwinick.com/attorneys/caleb-j-brus>



2


2



Agenda

- ERISA Background
- Origin & Evolution
- Common Violations
- Fiduciary Duties
- Cybersecurity Considerations
- Trends
- Questions

3



Background

4



Background

- ERISA is short for the Employee Retirement Income Security Act of 1974.
- Paternalistic federal law designed to protect the interests of employees and beneficiaries participating in private-sector retirement and health plans.
- Three primary principles:
 - Promoting informed financial decision-making,
 - Preventing mismanagement and abuse of benefit programs, and
 - Protecting reliance of participants and beneficiaries.

5

5



6

6



Tax Qualification

- Most plans intend to achieve special tax treatment.
- The preferential tax treatment is both the “carrot” and the “stick.”
- Failure to follow rules risks the tax qualification of the entire plan.
- Three major components of preferential tax treatment:
 - The employer receives a current deduction for amounts contributed to the plan,
 - The trust is generally exempt from taxation on its investment income, and
 - Money contributed by participants is not included in gross income until distributed by the plan.

7

7




Coverage

- ERISA generally preempts state laws.
- Applies to private sector plans (with exceptions) and generally applies to:
 - Defined Benefit Plans
 - Defined Contribution Plans
 - Welfare Benefit Plans
- Generally, excludes:
 - Governmental Plans
 - Church Plans
 - Non-U.S. Plans

8

8




Plan Document

- Governs the terms of the retirement plan.
- Most be closely adhered to.

9

9



Summary Plan Description (SPD)

- Plain language overview of the legal plan document.
- Generally, will prevail when the legal plan document and SPD conflict.

10

10



Other Participant Disclosures

- Strict participant disclosure requirements to ensure that employees are well-informed about their rights, benefits, and management of their benefit plan.
- Summary of Material Modifications; Summary Annual Report; Benefit Statements; Fee Disclosures; Blackout Periods; QDIA, etc.

11

11



Prohibited Transactions

- A fiduciary is prohibited from causing the plan to engage in a transaction with a party-in-interest if the fiduciary knows or should know that the transaction involved a direct or indirect sale, exchange or leasing of property, lending of money or credit, or furnishing of goods or services, or facilities between the plan and the party-in-interest.

12

12



Prohibited Transaction Exemptions

- Party-in-interest transactions are a broad prohibition so PTEs were created to allow for these transactions. For example, a participant loan is a PT because it involves a loan to a party-in-interest, the plan participant.
- There are statutory PTEs and individual PTEs. Participant loans are an example of a statutory PTE.

13

13

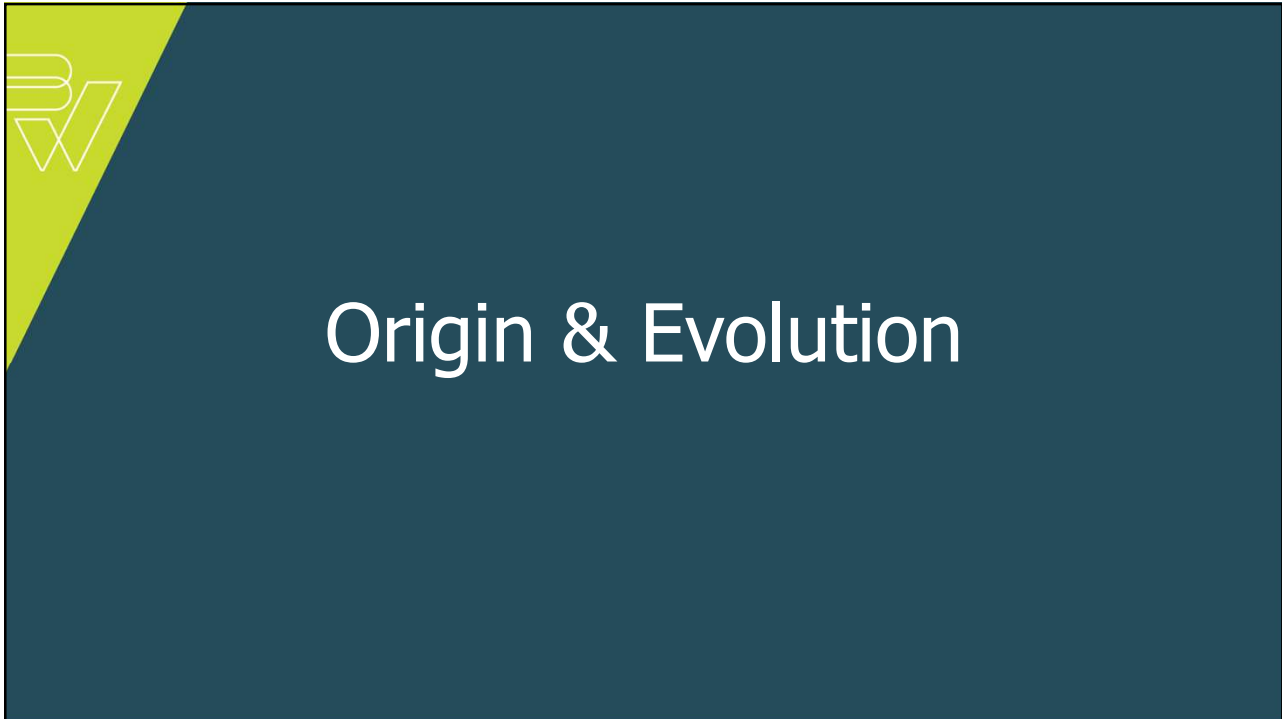


Accumulation Rules

- Ensure that employees can accumulate benefits, primarily focusing on eligibility, vesting, contribution limits, and non-discrimination.

14

14




15

A slide with a white background and a dark teal triangle in the top-left corner containing a yellow logo. The logo consists of a stylized 'B' and 'W' intertwined. The title 'Origins of ERISA' is centered in dark teal text. Below the title is a bulleted list of four points. The number '16' is in the bottom right corner.

- Collapse of Studebaker Corporation.
- Established minimum standards for participation, vesting, benefit accrual, and funding.
- Imposed strict fiduciary responsibilities on those who manage and control plan assets.
- Mandates important information to participants and beneficiaries.

16

16



Evolution of ERISA

- Introduction of 401(k) plans in the 1980s.
- Decline in defined benefit plans.
- Pension Protection Act of 2006.
- SECURE Act & SECURE 2.0.


17

17



Common Violations

18



Common ERISA Violations

- Failure to adhere to fiduciary standards.
- Mismanagement of plan assets.
- Failure to follow terms of the plan.
- Failure to fully correct errors.

19

19



ERISA Fiduciary Duties

20



Who is a Fiduciary?

- Any person who exercises discretion with respect to the management or administration of the plan or the management or disposition of plan assets.
- While certain titles convey a fiduciary status, title alone does not dictate whether someone is a fiduciary.

21

21



Fiduciary Duties

- Duty of Care (Prudence).
- Duty of Loyalty.
- Duty of Diversification.
- Duty to Follow the Terms of the Plan Document.

22

22



Duty of Care (Prudence)

- The “prudent person” standard is the universal standard of fiduciary conduct.
- Fiduciaries must act with the care, skill, prudence, and diligence that a prudent person would use in similar circumstances.

23

23



Duty of Loyalty

- The duty of loyalty requires fiduciaries to act solely in the best interest of plan participants and beneficiaries.
- Fiduciaries must avoid conflicts of interest.
- Fiduciaries must not advance their interests, or the interests of others, above the interests of participants and beneficiaries.
- Fiduciaries may not favor one group of participants or beneficiaries over another.

24

24



Duty of Diversification

- Fiduciaries must diversify plan assets to avoid the risk of large losses unless it is more prudent not to do so.

25

25




Duty to Follow the Terms of the Plan Document

- Fiduciaries must follow and administer the plan in accordance with the terms of the plan document.

26

26



Right of Delegation

- Fiduciaries may delegate duties to other professionals.
- Delegation does not make a fiduciary any less of a fiduciary.
- Fiduciaries retain the duty to monitor those to whom they have delegated responsibilities, and fiduciaries have a duty of reasonable inquiry into the actions of those persons.

27

27



Cybersecurity Considerations

28



Why Cybersecurity Matters for ERISA Plans

- ERISA Fiduciaries must act prudently in protecting plan assets, including digital data. Fiduciaries are responsible for:
 - Selection and monitoring of service providers for cybersecurity risks.
 - Continuous evaluation of the effectiveness of cybersecurity practices.
- Targeting of retirement plans.
 - Estimated that ERISA covers 2.8 million health plans, 619,000 other welfare plans, and 765,000 private pension plans.
- Integration of plan operations and technology.

29

29



Common Cybersecurity Threats

- Phishing attacks – attempts to deceive individuals into providing sensitive information.
- Ransomware – disrupting access to critical plan data.
- Insider threats – unauthorized access by employees or service providers.
- Third-party risks – breaches through vendors or service providers.

30

30



DOL's Cybersecurity Guidance (Sept. 2024)



Best practices for plan sponsors:

Develop a comprehensive cybersecurity program.
Conduct risk assessments regularly.
Engage with service providers that have strong cybersecurity policies.



Cybersecurity Program Best Practices:

Implement access control and identity management.
Ensure data encryption and secure system operations.
Regularly monitor and update security measures.




Online Security Tips for Participants:

Use strong passwords and multi-factor authentication.
Be cautious of phishing and suspicious emails.

31

31



Service Provider Oversight

- Conduct thorough due diligence.
- Determine how the service provider identifies, assesses, and manages risks.
- Ask about past breaches/incidents.
- Assess qualifications and track record.
- Review internal and external security reviews.
- Review insurance coverage for cyber security incidents.

32

32



Incident Response Expectations

- Inform law enforcement.
- Notify insurer.
- Investigate.
- Give affected plans & participants necessary info.
- Honor contractual requirements.
- Fix root cause.

33
33

33



Incident Response Plan



Preparation

Develop and train response teams
Establish communication protocols
Deploy tools and resources



Detection & analysis

Monitor systems
Classify incidents based on severity and type
SCOPE & impact



Containment, eradication & recovery

Limit spread
Remove the root cause (e.g., malware, unauthorized access)
Restore effected systems



Post incident activities

Debrief each incident
Update the program as needed.
Documentation!

34
34

34



Audits & Assessments

- Identify, assess and document how cybersecurity threats are evaluated and categorized.
- How does the cybersecurity program mitigate or accept the risks identified? TAKE ACTION!!
- How do controls change with changes in info systems?
- 3rd party audits (e.g., SOC2 Reports).

35
35

35



Contractual Agreements

- Carefully review and negotiate all 3rd party service contracts.
 - Review & negotiate definition of a cybersecurity incident.
 - Establish the incident notification timeframe obligations.
 - Determine how the service provider makes the plan and participants whole.
 - Determine if other guarantees or protections exist (e.g., customer protection guarantee).
 - Review and negotiate insurance requirements.

36
36

36



System Changes & Updates

- Don't overlook this potential source of incidents.
- Ensure regression testing is in place.
- Complete regression testing before release whenever possible.
- Does the change/update impact a tested control?
 - Don't lose sight of SOC reports, risk assessments and other assessments.

37

37



Data Minimization

- More data \neq better.
- Limit data to what is necessary, including what you share with service providers.
- Redact data where possible.
- Limit data retention.
- Ensure data purging.
- Avoid data in development and testing.

38

38



Access Management

- Ensure all access necessary.
- Ensure access type is appropriate (e.g., view vs edit).
- Implement dual control for certain transactions or transaction levels.
- Monitor activity of authorized users.
- Ensure access is removed upon termination.

39

39

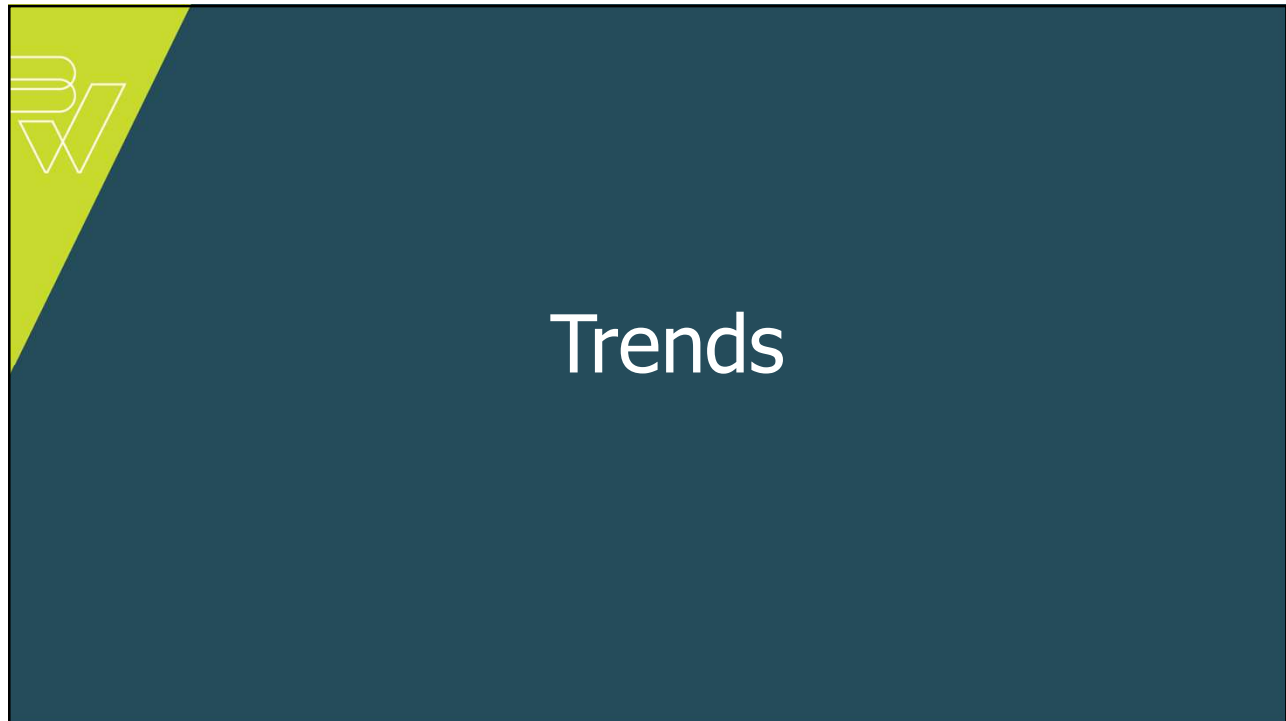


Participant Education

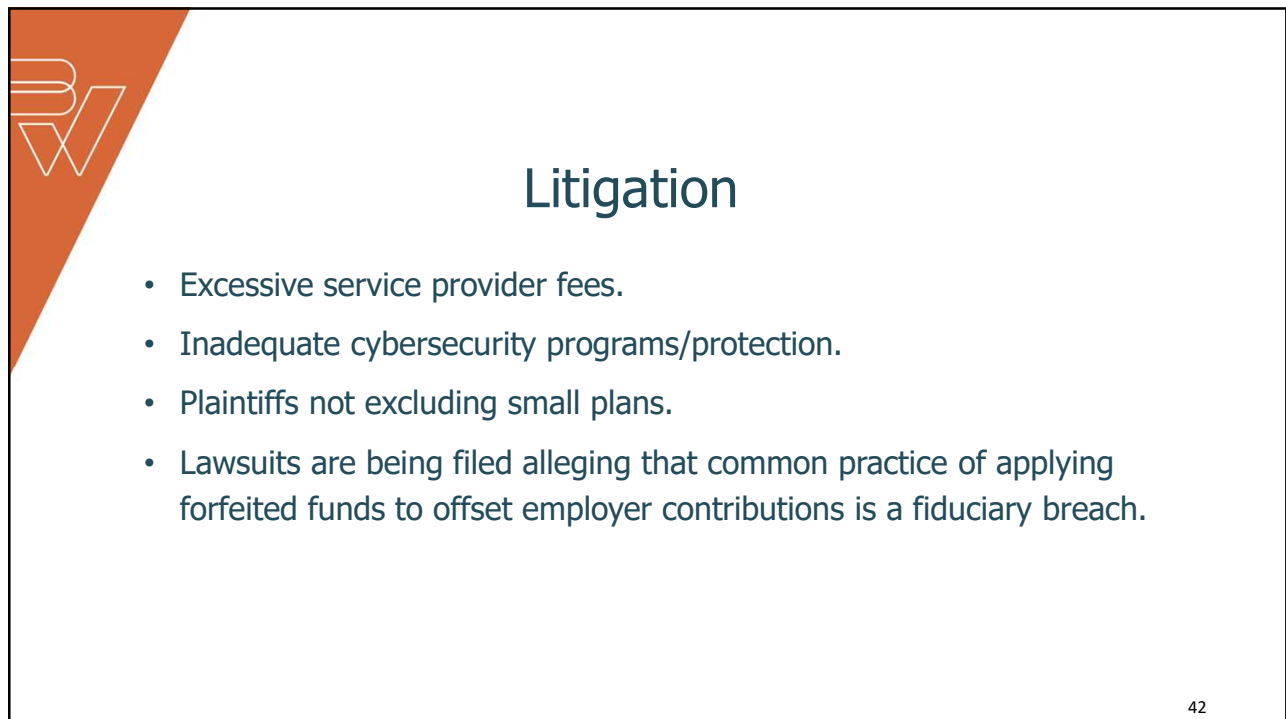
- Likely largest financial asset.
- Authenticate online accounts. Staying off the web does not prevent web attacks.
- Set alerts/check accounts regularly.
- Strong passwords & multifactor authentication.
- Keep personal info current.
- Avoid free Wi-Fi.
- Know how to report suspicious activity.

40

40



41



- Excessive service provider fees.
- Inadequate cybersecurity programs/protection.
- Plaintiffs not excluding small plans.
- Lawsuits are being filed alleging that common practice of applying forfeited funds to offset employer contributions is a fiduciary breach.

42

42



43