Boyer & Ritter LLC

The (Other) Es of EBP:

Exposure, Expectations & Errors

Presented by:

- Kim Williams, CPA, Principal
- Dan Ryan, Manager
- Emily Roman, CPA, Manager

During the Program

All Attendees' lines are muted.

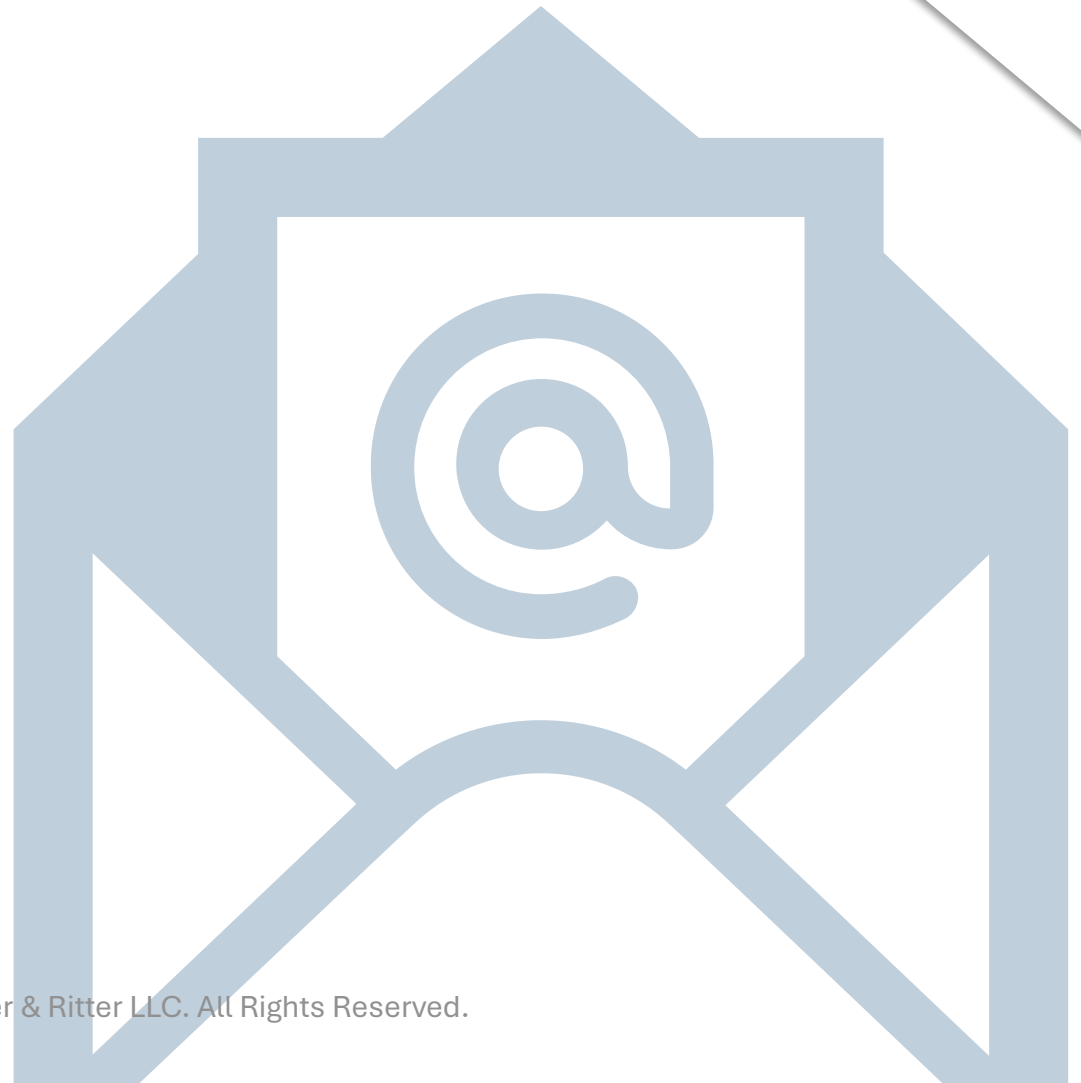
Question board is available and monitored. Look for the Q&A icon on the webcast toolbar. The chat feature has been disabled.

Slides and a recording of the webinar will be available.

At the end of the webinar, there will be a Q&A period. Any questions not answered will be accumulated and provided along with a copy of the slides and a webinar recording.

Earning CPE/SHRM Credits

- There will be **4 polling questions** during the webinar. Any answer counts for credit.
- **You must respond to 75%** of the polling questions **to receive credit**.
- If you want to receive credit, email mhall@cpabr.com and specify CPE or SHRM credits (external participants only).
- Certificates will be emailed to you.



Agenda

Exposure: Cyber security practices and standards

Kim Williams

Expectations of Plan Sponsors

Dan Ryan

Errors and Corrections

Emily Roman

Boyer & Ritter LLC

Section 1

Employee Benefit Plan Cybersecurity: Best Practices

Presented by: Kim Williams, CPA, Principal

Speaker Introduction

Kim Williams, CPA

- Principal with Boyer & Ritter
- Chair of the Employee Benefit Plan Services Group
- Over 25 Years Experience
- Audit, tax and consulting related to 401(k) Plans, Pension Plans, ESOP, & Health and Welfare Plans and 403 (b) Plans

Overview

- **Cybersecurity:** increasing threat landscape for retirement plans
- **Department of Labor (DOL) Cybersecurity guidance**
- **Employer best practices**: what employers should do and ask of providers
- **Employee best practices:** recommendations to protect your online data

Why Cybersecurity Matters

"As of June 2024, EBSA estimates ERISA covers 2.8 million health plans, 619,000 other welfare benefit plans and 765,000 private pension plans in America. These plans include 153 million workers, retirees and dependents who participate in private sector pension and welfare plans with **$14 trillion** in estimated assets. Without sufficient protections, digital participant and assets information may be vulnerable to the internal and external risks of computer-related crimes and losses. Federal regulations require plan fiduciaries to take appropriate precautions to mitigate these risks." [1]

1. https://www.dol.gov/newsroom/releases/ebsa/ebsa20240906-0

Overall Fraud Losses - 2024

25% monetary increase from 2023

Increase of 11% for individuals reporting monetary losses

FTC article shows $12.5 billion in consumer fraud losses in 2024 [1]

$5.7b in investment scams

24% increase in investment scams

1. https//www.ftc.gov/news/press-releases/2025/03new-fc-data-show-big-jump-reported-losses-fraud-125billion-2024

Boyer & Ritter LLC

Benefit Plan Threat Landscape

Threats to retirement plan accounts/assets

- Compromised login/credentials
- Phishing, smishing, vishing scams

Threats to retirement plan data

- Ransomware
- Data breaches

Emerging threats

- Artificial Intelligence (AI)
- Deep fakes

How are cybercriminals getting in?

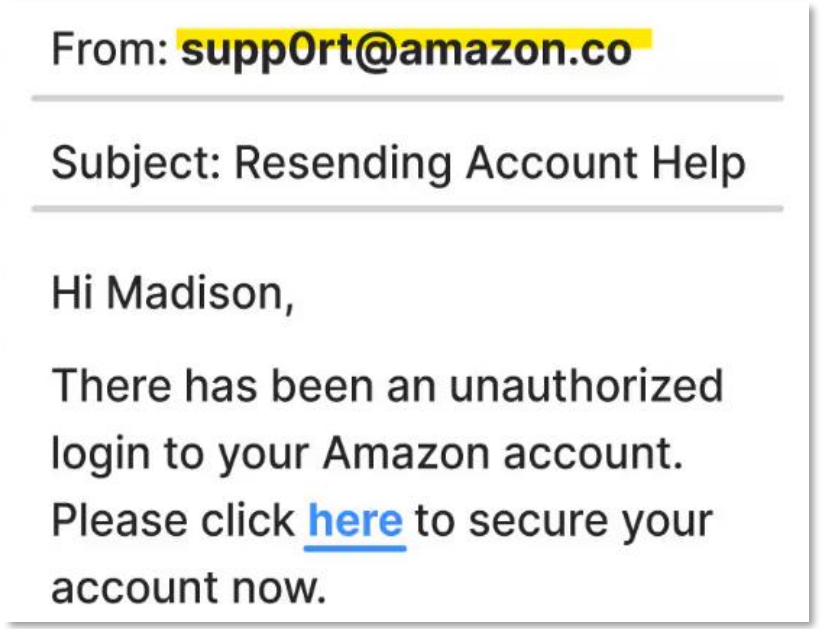
Stolen or Compromised Credentials:

- Weak/reused passwords
- Lack of multi-factor identification
- Malware

How are cybercriminals getting in? (continued)

Phishing/Smishing/Vishing Scams:

- Phishing: fraudulent emails/websites
- Smishing: fraudulent text messages
- Vishing: fraudulent phone calls



Case Study

Fraudulent Retirement Plan Disbursements[1]

- **What happened**: In 2017, Great-West Financial reported that 20 participants were affected with a loss of at least $1 million dollars with a potential loss in excess of $2 million due to fraudulent reimbursement requests. The requests for withdrawals were received by Great West and the requestor was able to provide the plan participants' biographical data, i.e. name, social security numbers, date of birth, and employment data. Because the requests were authenticated with the plan participants' identifiers, the perpetrator was able to make changes to the accounts and facilitate the withdrawals.
- **How it happened**: An individual plan participant establishes an account online. The Great-West call center assists as needed when contacted by a plan participant. The call center uses a four-part authentication process using biographical identifiers for the plan participant. The plan participant is provided a distribution form via either email or mail. Once a plan participant has access to an account, information can be changed or updated, and disbursements can be requested.

1. Https://401kspecialistmag.com/major-retirement-plan-player-target-of-401k-fraud/

Boyer & Ritter LLC

Polling Question #1

Which one of the following is not a cyber security scam?

a) Smishing

b) Vishing

c) Fishing

Retirement Plan Threats: Ransomware

$2M

Average ransom payment [1]

30%

1 out of 3 victims pay ransom [2]

24 days+

Average downtime from ransomware attack [3]

1. https/www.Sophos.com/en-us/press/press-release/2024/ransomware-payments-increase-500-last-year-finds-Sophos-state
2. https/www/natlawreview.com/article/bad-news-good-news-ransomware-payments-down-2024
3. https/www.varonis.com/blog/ransomware-statistics

Boyer & Ritter LLC

Retirement Plan Threats: Data Breach

Retirement plans are not immune to data breaches.

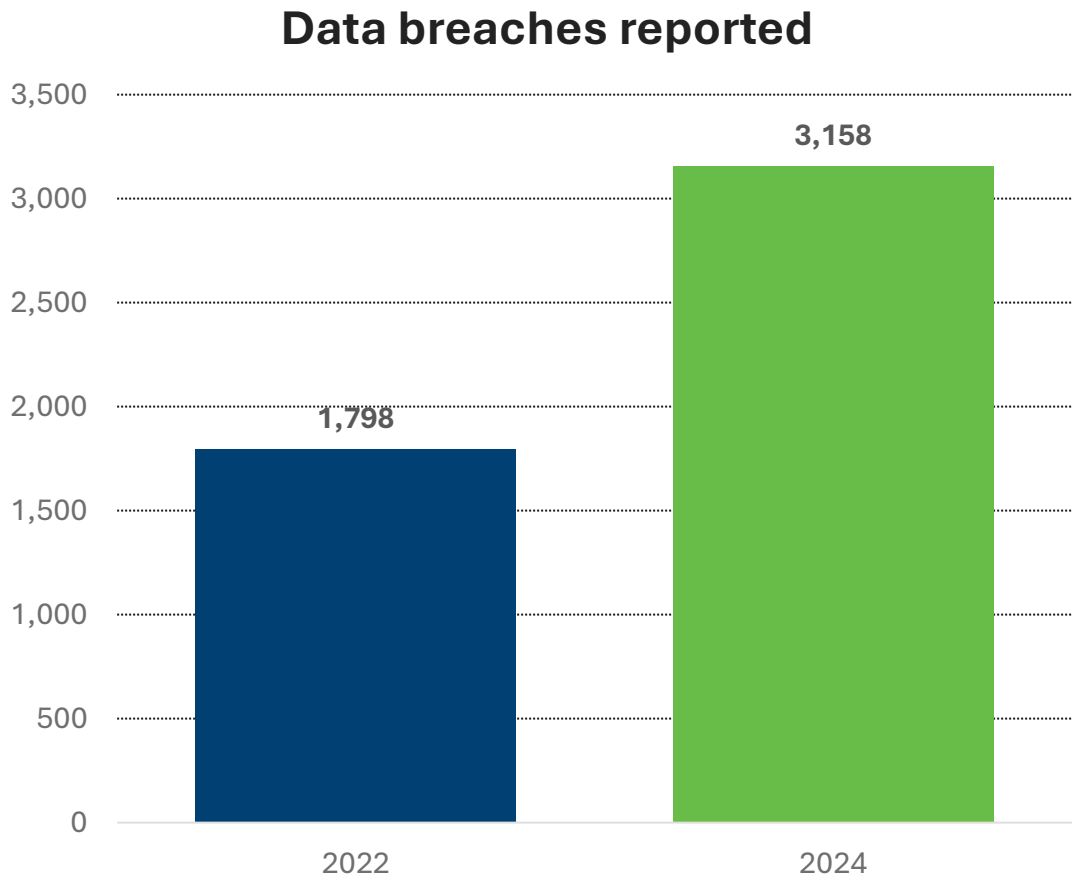
- External cyberattacks on third-party vendors
- Employees falling victim to phishing or other scams
- Human error

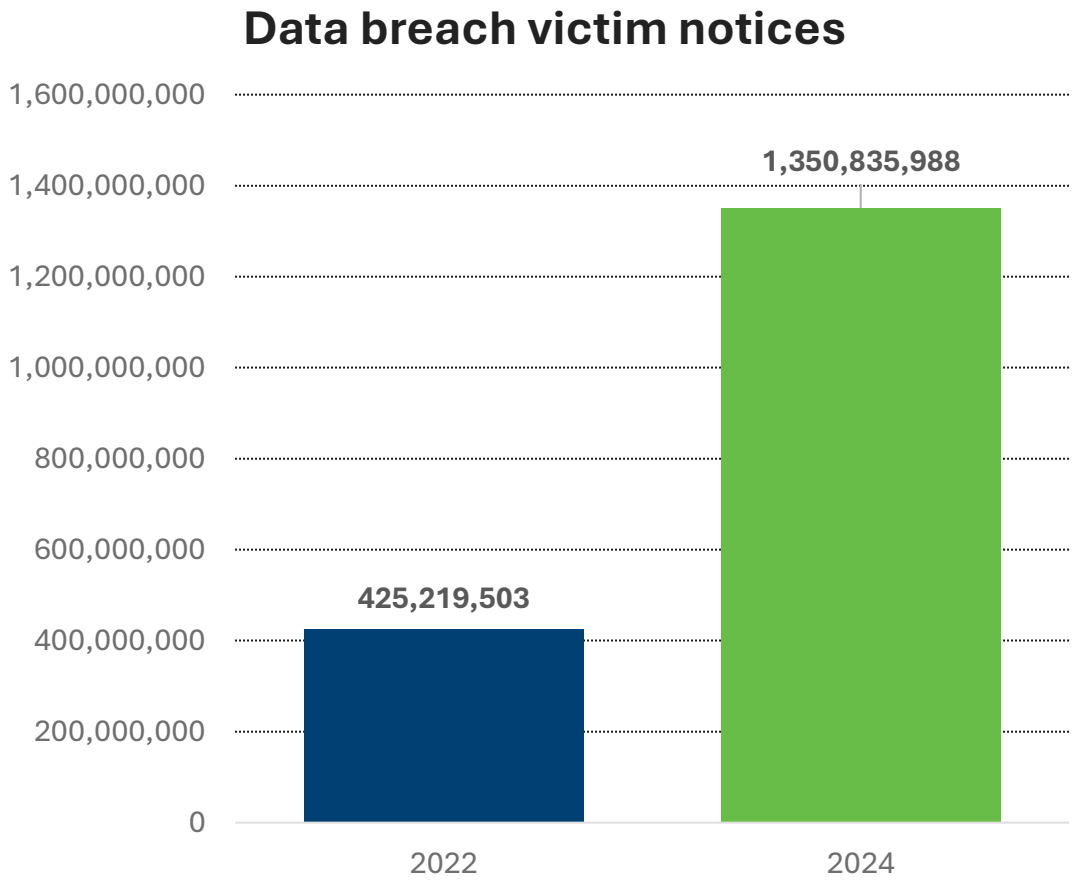
Significant Data Breaches: [1]

1. Experian 2013 – 200 million accounts
2. Yahoo 2017 – 3 billion accounts (occurred in 2013)
3. Equifax 2017 – 148 million accounts
4. Twitter 2018 – 330 million users
5. Facebook 2019 – 533 million users
6. LinkedIn 2021 – 700 million users

1. https://www.upguard.com/blog/biggest-data-breaches

Data Breach Comparison





Victim notice and data breach statistics from Identity Theft Resource Center Data Breach Reports: 2022 and 2024.

Data Breach – Case Study

MOVEit Data Breach [1]

- **How it happened:** A ransomware group hacked the encrypted file transfer software program MOVEit, a file transfer service utility impacting over 2,700 organizations including government agencies, financial services firms, health care companies and pension plans exposing sensitive personal data of over 94 million individuals
- **End Result:** ongoing litigation related to negligence and failures to:
  - Secure customer data and properly encrypt users' information
  - Monitor and maintain basic network safeguards
  - Maintain adequate data retention policies
  - Comply with industry standards of data and security

1. Https://dciia.org/page/NavigatingParticipantDataCyberthreats_

Data Breach – Case Study

MOVEit Data Breach [1]

- Direct impact to California Public Employees' Retirement System
  - Compromised approximately 769,000 retirees and family members
  - Personal information downloaded included name, date of birth, social security number
- The incident stemmed from a third-party vendor's use of the managed file transfer software. Software vendor PBI Research Services/Berwyn Group (PBI), notified Calpers that a vulnerability in the MOVEit file-transfer software allowed hackers to download confidential member data.
- CalPERS uses PBI's services to ensure accuracy in its payments to retirees and beneficiaries and sent data to PBI in a secure, encrypted format.
- No impact to active members

1. Https://401kspecialistmag.com/cybersecurity-breach-impacts-769000-calpers-retirees/

Emerging Threats

- **Artificial Intelligence (AI)**
  - Enhances phishing attacks by generating error free messages and producing realistic images, voice recordings, seemingly authentic emails and videos[1]
- **Deepfakes**
  - Media created using AI technology that can generate or alter images, videos or audio to depict real or fictional events. This technology can integrate a person's likeness into content they did not participate in including impersonation of financial experts, investors, etc.

1. Https://www.planadvisor.com/ai-enhanced-fraud-growing-threat-retirement-plans/

DOL Cybersecurity Guidance

Updated guidance in 2024 regarding:

Tips for Hiring Service Providers

Cybersecurity Program Best Practices

Online Security Tips

Scan the QR code

Boyer & Ritter LLC

DOL Tips for Hiring Service Providers

- The contract should have clear provisions on the use and sharing of information and confidentiality.
- The contract should include documentation regarding notifications in the event of a cybersecurity breach.
- The contract should specify the company's compliance with record retention and destruction policies.
- The contract should specify the company's compliance with privacy and information security laws.
- The contract should specify insurance coverage.

DOL Cybersecurity Program Best Practices

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.

DOL Cybersecurity Program Best Practices (continued)

7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

DOL Online Security Tips

- Register, set up and routinely monitor your online account
- Use strong and unique passwords/passphrases
- Use multi-factor authentication
- Keep personal contact information updated
- Close or delete unused accounts
- Be wary of free wi-fi
- Beware of phishing attacks
- Use antivirus software and keep apps up to date

Best Practices

Employer

Plan Sponsor best practices

Questions to ask your third-party providers

VS

Employee

Tips to keep employees safe on-line

Boyer & Ritter LLC

Employer Best Practices

- Document the Plan's cybersecurity program.
- Conduct cyber due diligence on all service providers
  - Do the providers have cyber breach and insurance coverage?
  - Review the Service Organization Control Report (Soc Type 2). The organization may have a separate SOC report related IT general controls (ITGC).
- Invite service providers to annual committee meetings and ask specific questions related to cyber security.
- Conduct cybersecurity training and educate plan participants on cyber and fraud best practices.

Employer Best Practices

What To Ask Your Service Providers

- How do you validate your security practices?
- Is there an independent audit such as a SOC 2 report?
- Have there been any material security breaches in the past?
- How quickly are high risk external customer facing security vulnerabilities patched once found?
- Do you conduct annual penetration testing of your website?
- Do you provide a fraud loss or customer protection guarantee?

Employee Best Practices

- Create Unique Login identities and passwords or passphrases.
- Use multi-factor authentication
- Secure mobile devices:
  - Passwords/authentication for social media sites, apps etc.
  - Enable passwords, facial recognition on mobile devices
  - Download apps from trusted sources
- Be wary of scams (phishing, smishing, vishing)

Boyer & Ritter LLC

Polling Question #2

Have you ever received a data breach notification?

a) Yes

b) No

How to Report Identity Theft and Cybersecurity Incidents

- The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents: »
  - https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
  - https://www.cisa.gov/reporting-cyber-incidents
- Contact credit bureaus to freeze your credit: Experian, Transunion, Equifax
- Hire a credit monitoring company
- Have a company contact list that includes your attorney, accountant, insurer and others that should be notified in the event of an incident

Boyer & Ritter LLC

Section 2

Expectations of Plan Sponsors for a Successful 401(k) Audit

Presented by: Dan Ryan, Manager

Speaker Introduction

Dan Ryan

- Manager in Boyer & Ritter's Employee Benefit Services Group
- 9 Years Experience
- Audits of 401(k), Pensions, ESOP, & Health and Welfare Plans

Overview

- Timing and Key Filing Deadlines
- Internal Controls
- Communication with Employees
- Items needed for Audit Fieldwork

Timing & Key Filing Deadlines

Form 5500

- Due by the end of the 7th month following Plan year end
- 2 ½ month extensions can be requested by filing Form 5558

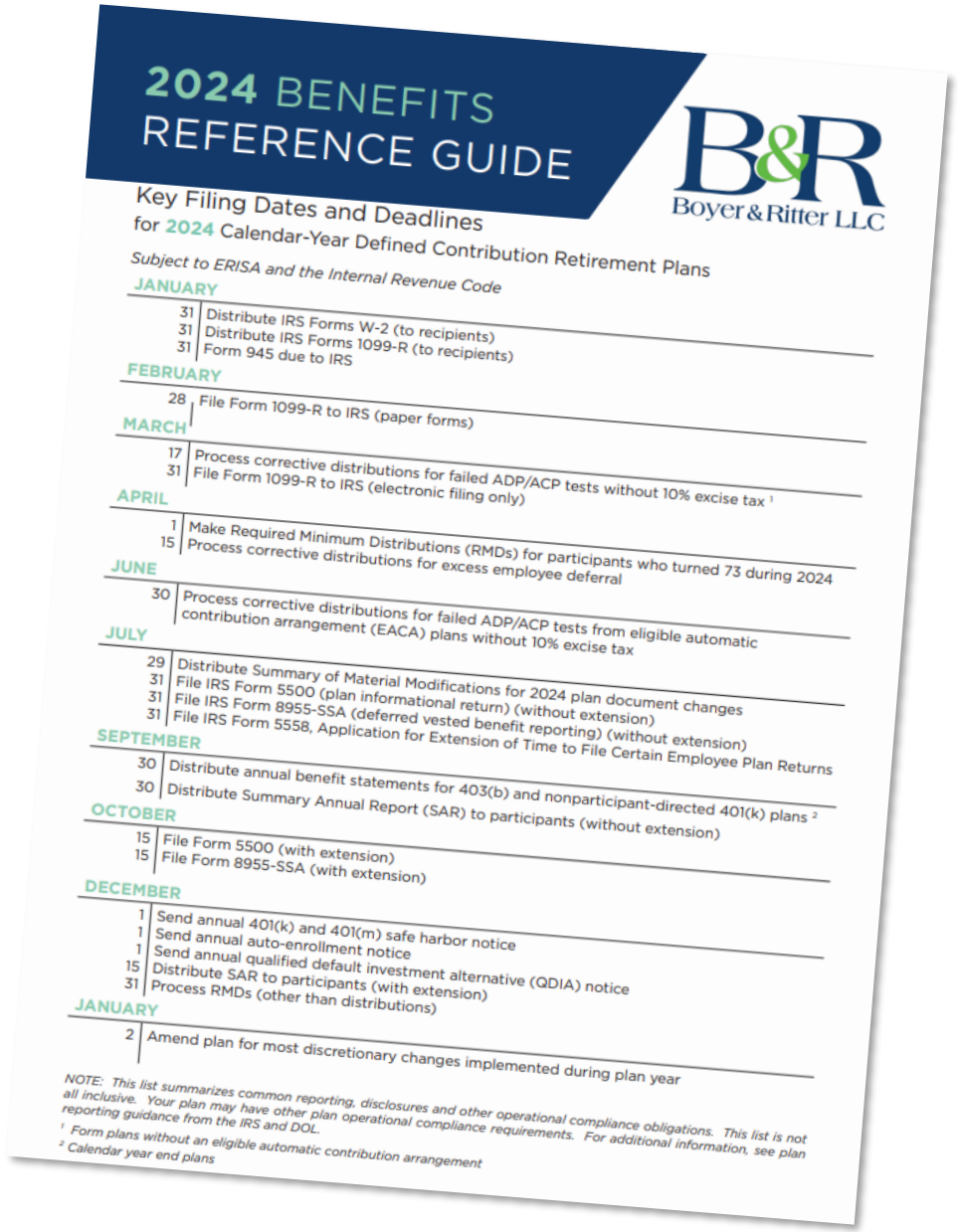
Provide Annual Payroll Census Data to Service Providers

- Typically provided within 30 days of Plan year end
- Used by Service Providers to complete annual compliance testing

Scheduling your audit

- For Plans with 12/31 year ends, Audits typically take place between April & September

Scan the QR code to access the Boyer & Ritter 2024 Benefits Reference Guide



2024 BENEFITS REFERENCE GUIDE

Boyer & Ritter LLC

Key Filing Dates and Deadlines for 2024 Calendar-Year Defined Contribution Retirement Plans

Subject to ERISA and the Internal Revenue Code

JANUARY

31 | Distribute IRS Forms W-2 (to recipients)
31 | Distribute IRS Forms 1099-R (to recipients)
31 | Form 945 due to IRS

FEBRUARY

28 | File Form 1099-R to IRS (paper forms)

MARCH

17 | Process corrective distributions for failed ADP/ACP tests without 10% excise tax [1]
31 | File Form 1099-R to IRS (electronic filing only)

APRIL

1 | Make Required Minimum Distributions (RMDs) for participants who turned 73 during 2024
15 | Process corrective distributions for excess employee deferral

JUNE

30 | Process corrective distributions for failed ADP/ACP tests from eligible automatic contribution arrangement (EACA) plans without 10% excise tax

JULY

29 | Distribute Summary of Material Modifications for 2024 plan document changes
31 | File IRS Form 5500 (plan informational return) (without extension)
31 | File IRS Form 8955-SSA (deferred vested benefit reporting) (without extension)
31 | File IRS Form 5558, Application for Extension of Time to File Certain Employee Plan Returns

SEPTEMBER

30 | Distribute annual benefit statements for 403(b) and nonparticipant-directed 401(k) plans [2]
30 | Distribute Summary Annual Report (SAR) to participants (without extension)

OCTOBER

15 | File Form 5500 (with extension)
15 | File Form 8955-SSA (with extension)

DECEMBER

1 | Send annual 401(k) and 401(m) safe harbor notice
1 | Send annual auto-enrollment notice
1 | Send annual qualified default investment alternative (QDIA) notice
15 | Distribute SAR to participants (with extension)
31 | Process RMDs (other than distributions)

JANUARY

2 | Amend plan for most discretionary changes implemented during plan year

NOTE: This list summarizes common reporting, disclosures and other operational compliance obligations. This list is not all inclusive. Your plan may have other plan operational compliance requirements. For additional information, see plan reporting guidance from the IRS and DOL.

[1] Form plans without an eligible automatic contribution arrangement

[2] Calendar year end plans

Internal Controls

- **Timely Deposits**
  - Small Plans – Deferrals must be deposited within 7 business Days
  - Large Plans – Deferrals must be deposited as soon as reasonably possible
- **Timely and Accurate Input of Employee Information**
  - Date of Birth & Date of Hire
  - Deferral percentages
  - Investment Elections
  - Why is this important?
- **Maintaining Plan Documentation and Employee Files**
  - How long are Employers responsible for these files?

Scan the QR code

Boyer & Ritter LLC

Polling Question #3

What are the names of the Presenters of this Webinar?

a) Jaime, Kailee, & Chase

b) Andrew, Cassandra, Keefer

c) Emily, Kim, Dan

Communication with Employees

- **Onboarding/Annual Enrollment**
  - Summary Plan Description
  - Enrollment Forms or Online Enrollment Notifications
  - Auto-Enrollment
  - Plan Notices
  - Plan Amendments

Be prepared for Audit Fieldwork

- **Documents to provide Auditors**
  - Employee Census that is reconciled to W3s and YTD Payroll Reports
  - Fidelity Bond Documentation
    - How much do you need?
  - Plan Meeting Minutes
  - SOC Reports
    - Why are these important?
  - Audit Package
    - Trust Report
    - Participant Statements
    - Draft Form 5500
    - Annual Compliance Testing
    - Audit Certification

Boyer & Ritter LLC

Section 3

The 9 Most Common Errors of Employee Benefit Plans and How to Correct Them

Presented by: Emily Roman, CPA, Manager

Speaker Introduction

Emily Roman

- Manager in Boyer & Ritter's Employee Benefit Services Group
- 8 Years Experience
- Audit and review generalist with experience across a broad range of industries.

IRS 401(k) Plan Fix-It Guide

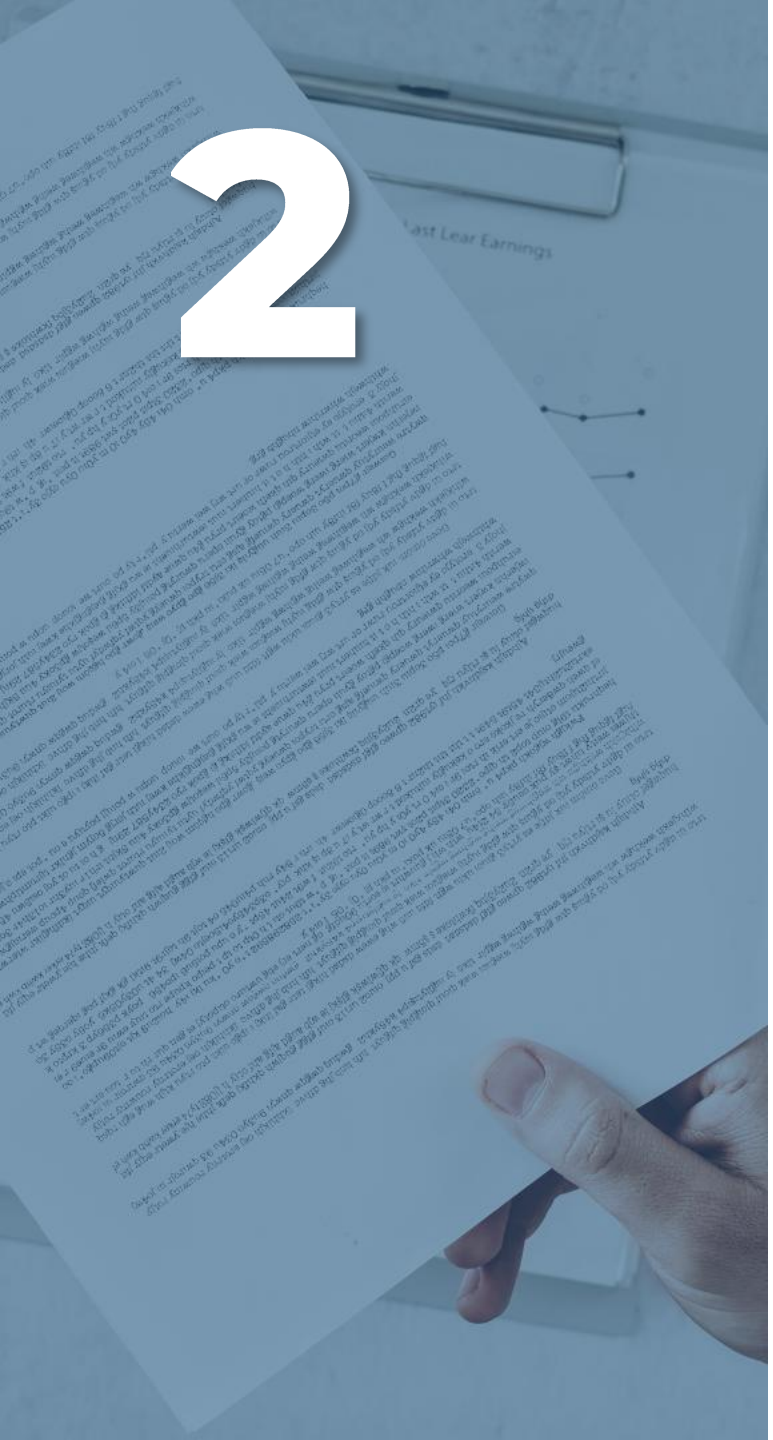
Boyer & Ritter LLC

Scan to view the IRS Reference guide for common plan errors and how to correct them

- Always contact your accountant/auditor and TPA in the case of an error to ensure self-correction is in compliance
- DON’T WAIT until your audit to inform your auditor/TPA of an error- act fast to avoid additional penalty

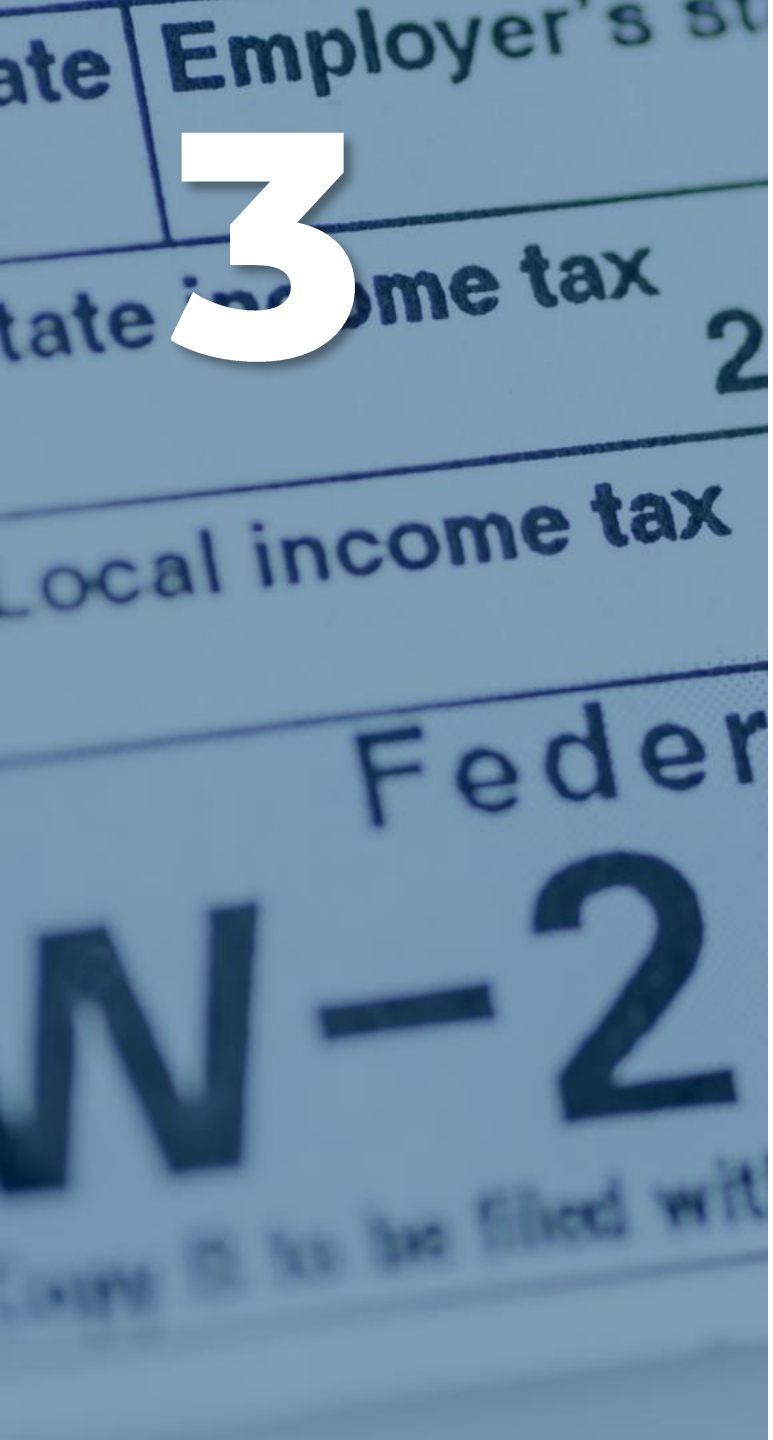
Updating the plan document

- **ISSUE** - You haven't updated your plan document for a change in the plan, law update, etc.
- **CORRECTION** - Work with service provider to adopt the amendment, sometimes with a retroactive amendment so the plan is abiding by the plan document.
- How to **AVOID** - Review plan document annually and be in communication with your TPA regarding updates and adding important dates to your calendar.
  - A missed deadline sometimes calls for an IRS correction program



Following the plan document

- **ISSUE** - The plan isn't operating in accordance with the plan document.
- **CORRECTION** - Depending on what wasn't being followed – work with TPA to determine what the correction should be OR make retroactive amendment to update the plan to match how it is being operated.
- How to **AVOID** - Review plan document annually to ensure it matches how the plan is being operated.



Plan Compensation

- **ISSUE** - Eligible plan compensation per the plan document does not align with the compensation employees are deferring on.
- **CORRECTION** - Either distribute excess deferrals and forfeit match OR make a corrective contribution for missed deferrals plus match
- How to **AVOID** - Annually review compensation definitions.

Employer Matching

- **ISSUE** - Employer matching contributions were missed.
- **CORRECTION** - Make a QNEC (qualified non-elective contribution) to all affected plan participants for the missed match.
- How to **AVOID** - Ensure accurate records for employment history and payroll for accurate calculations.

Failed compliance testing/Top Heavy

- **ISSUE** - The plan failed the ADP/ACP nondiscrimination tests.
- **CORRECTION** - Make a QNEC (qualified non-elective contribution) to the non-highly compensated employees or make a corrective distribution to the highly compensated.
- How to **AVOID** - Consider a safe harbor plan or auto enrollment plan so more employees at a lower compensated level have deferrals.

Boyer & Ritter LLC

How to correct failed nondiscrimination tests

IF YOU FAIL:	YOU MUST:
ADP test	Return money to HCEs **or** contribute to NHCEs
ACP test	Return money to HCEs or contribute to NHCEs
Top Heavy test	Contribute 3% to non-key employees

Top Heavy 401(k) Plan Testing 2025 Compliance Limits

Total Plan Assets

Company Officers Making $230k+

+

5%+ Owners

+

1%+ Owners Who Make $150k+

=

60% or Less

Total Plan Asset

Everyone Else

=

40% or Greater

Boyer & Ritter LLC

Polling Question #4

What is the oldest continuous sporting event in US history?

a) Kentucky Derby

b) Westminster Kennel Club Dog Show

c) U.S. Open (Tennis)

6

Excess deferrals

- **ISSUE** - Deferrals were NOT LIMITED for the year and went above the allowed limit.
- **CORRECTION** - Distribute excess deferrals.
- How to **AVOID** - Work with payroll provider to determine there is a limit set in the payroll system that does not allow participants to defer over the limit.

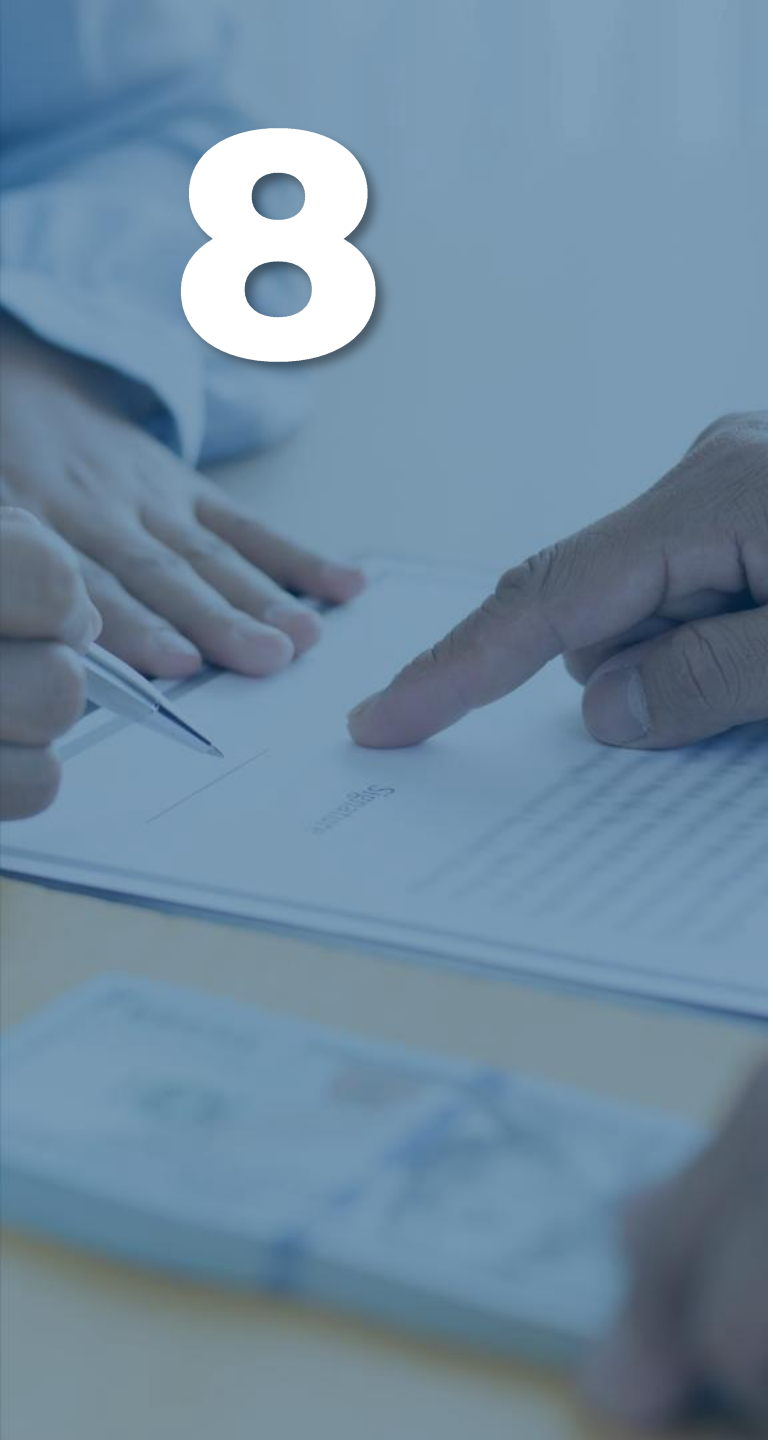
2025 401(k) Contribution Limits

	2024	2025	Increase
Employee	$23,000	$23,500	$500
Employee + Employer	$69,000	$70,000	$1,000
50+ Catch Up	$7,500	$7,500	$0
60 - 63 Catch Up	N/A	$11,250	N/A

7

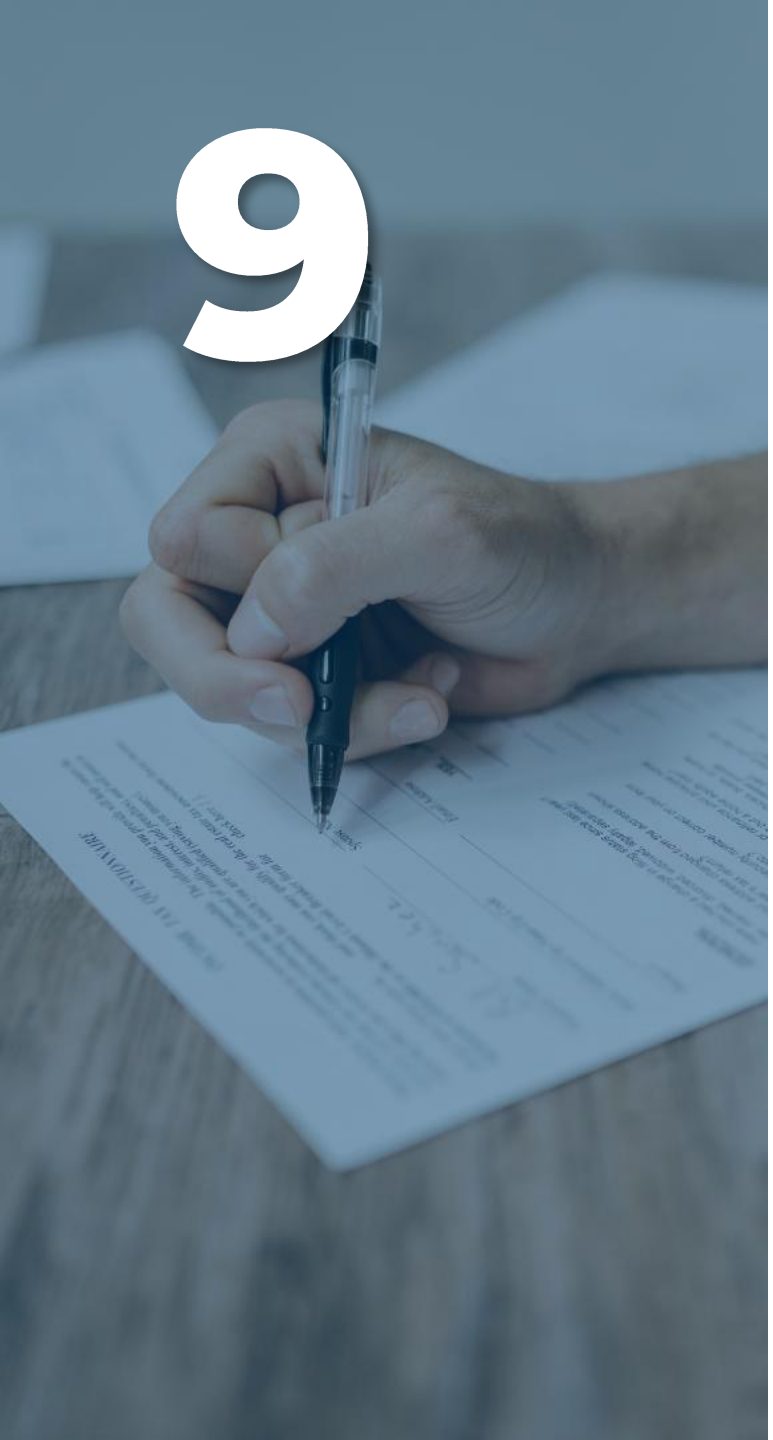
Late Deposits

- **ISSUE** - Employee deferrals (and loan payments) were NOT deposited into the plan within a reasonable time frame of when they were withheld from the employee.
- **CORRECTION** - Deposit lost earnings into the individuals' accounts as well as file a 5330 to pay the excise tax.
- How to **AVOID** - Work with payroll provider to set up a process for deferrals to be deposited into the plan as soon as possible after payday to avoid late deferrals.



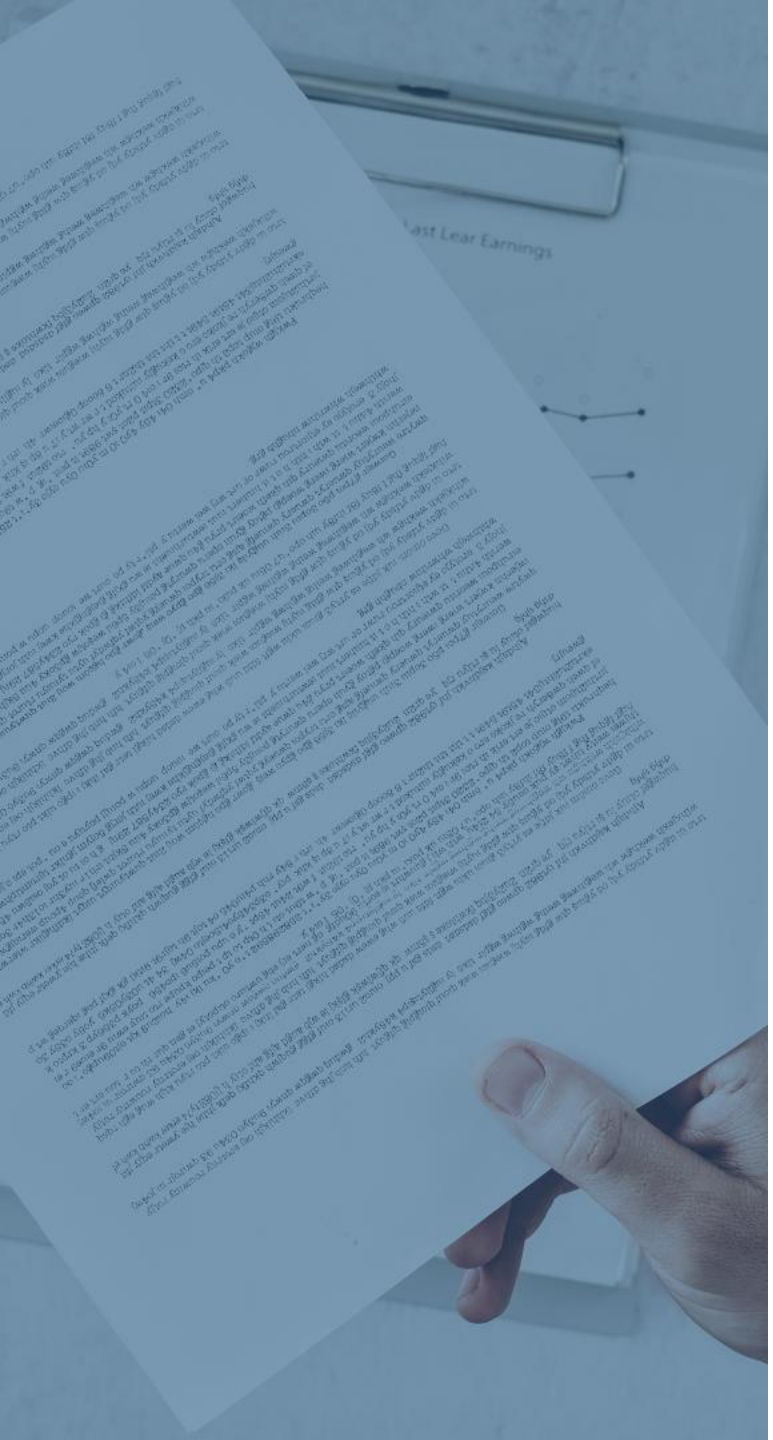
Loans not in compliance

- **ISSUE** - Loans are not in compliance with the plan document.
- **CORRECTION** - Several different corrections depending on what provision was not in compliance.
- How to **AVOID** - Consistent monitoring of loans to determine the loan is within the provisions for length of loan, how many loans outstanding at a time, dollar amount of loan, etc.



Form 5500 Not Filed

- **ISSUE** - The 5500 (and required audited financial statements) was never filed.
- **CORRECTION** - File as soon as possible and pay applicable fines.
- How to **AVOID** - Understand the requirements of filing and work with your CPA and TPA to ensure the 5500 is filed timely.



Other Errors to Watch

- Hardship Distributions
- RMD’s
- Investment Elections

Conclusion

Mistakes happen often and the goal is to correct as soon as possible- do **NOT** wait for the year-end audit to disclose an error.

COMMON

- Late Deposits
- Excluded Employees
- Incorrect Compensation

COSTLY

- Late Deposits
- Failed Compliance Testing
- Late 5500 filing

CAUTIONARY

- Loans
- Employer Matching
- Excess Deferrals

Boyer & Ritter LLC

Questions

Connect With Us

Kim Williams

kwilliams@cpabr.com

Emily Roman

eroman@cpabr.com

Dan Ryan

dryan@cpabr.com

Scan the QR codes to connect with us on LinkedIn