

General Session IV Fraud in Benefit Plans - How to Tell if There's a Hand in the Cookie Jar

Robert A. Lavenberg, CPA, JD, LL.M
President, ERISAworks, LLC

Paul T. Harger
*Supervisory Investigator, US Department of Labor -
Employee Benefit Security Administration (EBSA)*



November 9, 2018

ERISAworks, LLC



Fraud in Benefit Plans - How to Tell if There's a Hand in the Cookie Jar

Paul T. Harger, Supervisory Investigator, US Department of Labor - Employee Benefit Security Administration (EBSA)

Paul has more than 27 years of enforcement experience in the employee benefits field with an extensive background in both civil and criminal investigations. Currently, Paul is responsible for overseeing all criminal investigations for the Dallas Regional Office and serves as the primary liaison to other federal and state enforcement authorities involved in ERISA criminal investigations. Paul graduated from the University of Cincinnati with a B.B.A. in Accounting; and completed the Executive Potential Program offered by Graduate School USA.



harger.paul@dol.gov
72) 850-4532

Department of Labor -
Employee Benefit Security
Administration (EBSA)
Griffin, Suite 900
TX 75202 60606

www.dol.gov/ebsa



ERISAworks, LLC

Robert A. Lavenberg, CPA, JD, LL.M, CGMA

President - ERISAworks, LLC

EXPERIENCE SUMMARY

Bob Lavenberg has more than thirty years of experience with the Employee Retirement Income Security Act of 1974 (ERISA) and related business advisory services. His expertise spans reporting, government compliance and assessment of tax implications for plans, including qualified retirement, health, welfare, and fringe benefit plans. As a National Assurance Partner for an international accounting firm, Bob focused on employee benefit plan (EBP) audit quality for his clients and the firm's 1,900+ plans. Bob is a past chair of the American Institute of CPAs (AICPA) EBP Audit Quality Center and the two annual AICPA National EBP Conferences. Bob was also an active member of the AICPA's EBP Expert Panel. Bob has written articles for professional journals, contributed to internal employee benefit plan audit trainings and is a frequent speaker on various technical issues for industry and professional organizations.

PROFESSIONAL AFFILIATIONS

American Bar Association

American Institute of Certified Public Accountants

- Member, Council (2015-2017)
- Chair/Member, Employee Benefit Plan Audit Quality Center Executive Committee (2008 - 2013, 2016 - 2017)
- Chair, Joint 403(b) Plan Audit Task Force
- Member, Employee Benefit Plans Expert Panel (2005 - 2008)
- Chair - National Conference on Employee Benefit Plans Conference (2010 - 2011)
- Chair - Employee Benefit Plans Accounting, Auditing, and Regulatory Update Conference (2009 - 2011)

International Foundation of Employee Benefit Plans

Pennsylvania Institute of Certified Public Accountants

- Member, Employee Benefits Conference Committee
- Member, Ethics Committee (2006 - 2009)

New Jersey Society of Certified Public Accountants

- Member, Audit and Accounting Interest Group
- Vice-Chair, Employee Benefits Conference Committee (2017)

Society for Human Resource Management

US Department of Labor - EBSA - ERISA Advisory Council

EDUCATION

LL.M. in Taxation, Boston University

J.D., New England School of Law

B.S., Northeastern University



lavenberg@ERISAworks.com
Phone: 215-850-6288

ERISAworks, LLC
100 Fox Chase Drive
Plymouth, PA 19454

www.ERISAworks.com



Auditing Standard - Clarified (AU-C) Section 240

- *Consideration of Fraud in a Financial Statement Audit*
 - The distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the financial statements is **intentional** or unintentional
 - The auditor is primarily concerned with fraud that causes a **material misstatement** in the financial statements
 - The primary responsibility for the prevention and detection of fraud rests with both **those charged with governance** of the entity and **management**
 - An auditor is responsible for obtaining reasonable assurance that the financial statements as a whole are free from material misstatement, **whether caused by fraud or error**



Fraud Risk Factors - Fraudulent Financial Reporting

Incentive/Pressure	Opportunity	Attitude
Financial or other instability of sponsor	Management = governance	Tone at the top
Poor investment results	Significant estimates	A disregard for regulatory environment
Underfunded position	Lack of oversight	Overreliance on third parties
New requirements - accounting or regulatory	High turnover rates	Lack of transparency



Fraud Risk Factors - Misappropriation of Assets

Incentive/Pressure	Opportunity	Attitude
Known financial pressures for key plan employee	Lack of oversight	Changes in behavior or lifestyle
Employee dissatisfaction - more work, same pay	Limited segregation of duties	Disregard for internal controls
Promotions or other rewards inconsistent with expectations	Inadequate management understanding	Failure to correct deficiencies



Fiduciary Responsibility for Plan Data

■ Fiduciary

- *“An individual in whom another has placed the utmost trust and confidence to manage and protect property or money.”*
- *“The relationship wherein one person has an obligation to act for another's benefit.”*
- *ERISA requires the plan fiduciary to act as a “prudent fiduciary” - a person well versed in those requirements*



Fiduciary Responsibility for Plan Data

- 2016 ERISA Advisory Council Report
 - *Cybersecurity Considerations for Benefit Plans*
 - “... provide plan sponsors, fiduciaries and service providers with information on developing and maintaining a robust cyber risk management program for benefit plans.”
 - “... educate them on cybersecurity risks and potential approaches for managing these risks.”

<https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf>



Examples of Fraud

- American Institute of Certified Public Accountants (AICPA) Employee Benefit Plan Audit Quality Center (EBPAQC)
 - Publication - *EBP Fraud Examples*
 - Summary Analysis - *DOL Criminal Enforcement Cases*
 - Grouped by significant area
 - Distributions
 - Expenses/forfeitures
 - Participant loans
 - Eligibility
 - Contributions
 - Investments



DOL's Ten Warnings Signs That Your 401(k) Contributions Are Being Misused

1. Your 401(k) or individual account statement is consistently late or comes at irregular intervals - or not at all!
2. Your account balance does not appear to be accurate
3. Your employer failed to transmit your contribution to the plan on a timely basis



DOL's Ten Warnings Signs That Your 401(k) Contributions Are Being Misused

4. There was a significant drop in your account balance that cannot be explained by normal market ups and downs
5. 401(k) or individual account statement shows your contribution from your paycheck was not made
6. Investments listed on your statement are not what you authorized
7. Former employees are having trouble getting their benefits paid on time or in the correct amounts



DOL's Ten Warnings Signs That Your 401(k) Contributions Are Being Misused

8. Unusual transactions, such as a loan to the employer, a corporate officer, or one of the plan trustees
9. Frequent and unexplained changes in investment managers or consultants
10. Your employer has recently experienced severe financial difficulty



Examples of Fraud

- “Real-life” examples
 - Assistant Controller at a nonprofit organization was in charge of 401(k) plan activity
 - Authorized several plan loans on her own behalf, even though the plan limited the number of loans to one at a given time
 - Hackers used personal information of employees to set up online profiles on the plan custodian’s web platform
 - Requested loans worth \$2.6 million
 - 91 accounts were breached but only 58 had fraudulent loans disbursed



Examples of Fraud - Pension/401(k) Plans

- A CPA firm failed to deposit both employee contributions and employer matching contributions to the SIMPLE IRA Plan since 2015 totaling \$18,702
- An office manager for a construction company was stealing from the SIMPLE IRA Plan by depositing other participants' contributions into her personal account, and then withdrawing the funds
- A dental management company knowingly misapplied approximately \$109,945 of employee contributions by withholding them from participants' paychecks and then failing to forward them to Plan
- A hacker used personal information of a participant to gain access to his Plan account and withdraw \$60,000 as a hardship distribution; another hacker took a \$13,000 loan in which the participant is making loan repayments through payroll deductions



Examples of Fraud - Multiemployer Plans

- The son of a deceased beneficiary received benefit payments from August 2011 through February 2018 totaling \$39,829, which was intended for his mother who died on July 29, 2011
- A participant's wife submitted fraudulent pharmacy receipts to Health and Welfare Plan for reimbursement, which were altered to appear as though they were written for members of her family
- A sister of a participant knowingly accepted social security benefits, VA benefits and Pension Plan benefits of her deceased brother (8/22/2016), beyond the time of his death totaling \$18,507



Examples of Fraud - Service Providers

- A Third Party Administrator who provided services to pension plans was systematically submitting fraudulent distribution requests to the custodian for disbursements of retirement funds that were directed to their own operating account (approximately \$14.5 million). The TPA was maintaining fraudulent recordkeeping documents
- A Third Party Administrator who provided health insurance coverage through a PEO arrangement, failed to forward the premiums to the insurance carrier. As a result, the participating employers' insurance coverage was terminated and there are multiple outstanding claims. The funds were used for the owner's personal use and financial gains



Examples of Fraud - Health Plans/Health Care Fraud

- An Employer failed to remit \$210,915 in health premiums deducted from employee's salaries from April 2014 through December 2016. Although these funds were deducted from employee's salaries, the employer failed to remit them to the insurer. As a result, the insurance company terminated the health coverage retroactively, resulting in unpaid medical claims
- On November 16, 2016, a Federal Grand Jury located in the Northern District of Texas indicted 21 individuals involved in a massive criminal conspiracy to defraud fully insured and self-funded ERISA covered health plans, which were administered by UnitedHealthcare, Aetna, and CIGNA, in addition to government sponsored health care programs such as Medicare, Medicaid, FECA, TRICARE, and the FEHBP



Examples of Fraud - Health Care Fraud (continued)

- The conspiracy was executed through Forest Park Medical Center Dallas (FPMC), which was a physician owned, surgical hospital located in Dallas, Texas. FPMC paid approximately \$40 million in bribes and kickbacks to surgeons, primary care physicians, chiropractors, lawyers, workers' compensation preauthorization specialists, and others
- As a result of the bribes, kickbacks, and other inducements, FPMC billed such patients' insurance plans and programs well over half-a-billion dollars and collected over two hundred million dollars in paid claims, from approximately 2009 to 2013



Example Internal Controls to Mitigate Fraud

- Participant data:
 - Employee participation refusals ('opt-outs') are retained for future reference
 - Maintenance of participant data is segregated from responsibility for benefit approval or processing
 - All participant-initiated enrollments, transfers, changes in investment allocations, and other change requests must be authorized by the participant - 2-step verification
 - The ability to perform these activities electronically or directly with a third-party administrator is restricted to authorized participants through the use of specific identification and a personal identification number. Invalid attempts to access and perform functions are reviewed and investigated



Example Internal Controls to Mitigate Fraud

■ Contributions:

- Cash is independently controlled upon receipt
- Procedures are in place to monitor that cash receipts are deposited intact daily
- To prevent theft, checks are restrictively endorsed upon receipt
- Procedures are in place for the segregation of duties between the responsibility for receiving contributions and for the processing of contributions
- Bank and investment accounts are reconciled monthly
- Remittance Policy
 - Past-due contributions are investigated on a timely basis
- Secure access to computerized contribution records is limited to those with a logical need for such access



Example Internal Controls to Mitigate Fraud

■ Investments:

- Responsibility for investment decisions and transactions is segregated from the custodian's functions
- Financial stability of financial institutions holding investments is reviewed
- Written-off investments are reviewed for possible appreciation
- Documents are controlled in a limited-access, fireproof area
- Securities held by custodians are confirmed
- Secure access to computerized investment records is limited to those with a logical need for such access



Example Internal Controls to Mitigate Fraud

- **Benefit payments:**
 - Responsibilities for benefit approval, recording of benefits, and maintenance of participant files are adequately segregated
 - Blank forms are prenumbered and effectively controlled
 - Periodic correspondence with retired beneficiaries is maintained, and correspondence or payments are returnable to plan committee if undeliverable
 - Check endorsements are compared with signature in applicable participant records
 - Supporting documents are effectively canceled on payment
 - Secure access to computerized benefit payment records is limited to those with a logical need for such access



Communication Requirements

- AU-C section 260, *The Auditor's Communication With Those Charged With Governance*
- AU-C section 265, *Communicating Internal Control Related Matters Identified in an Audit*





QUESTIONS?

