



Association Fraud: How It Happens and What You Should Know

National Association Conference

September 17, 2015

Chicago, Illinois

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor. | ©2015 CliftonLarsonAllen LLP



Four Key Points

- I. Common and Clever Schemes Employees Use to Commit fraud Against Employer
- II. Warning Signs, Red Flags and Indicators of Predications of Theft or Abuse
- III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized
- IV. Recommendations to Consider when Suspicion of Fraud Exists



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer

- Fraud is defined as:

A false representation of a matter of fact—whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed.

- The fraud triangle is a model for explaining the factors that cause someone to commit occupational fraud. It consists of three components which, together, often lead to fraudulent behavior:
 1. Perceived unshareable financial need
 2. Perceived opportunity
 3. Rationalization



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer (cont'd)

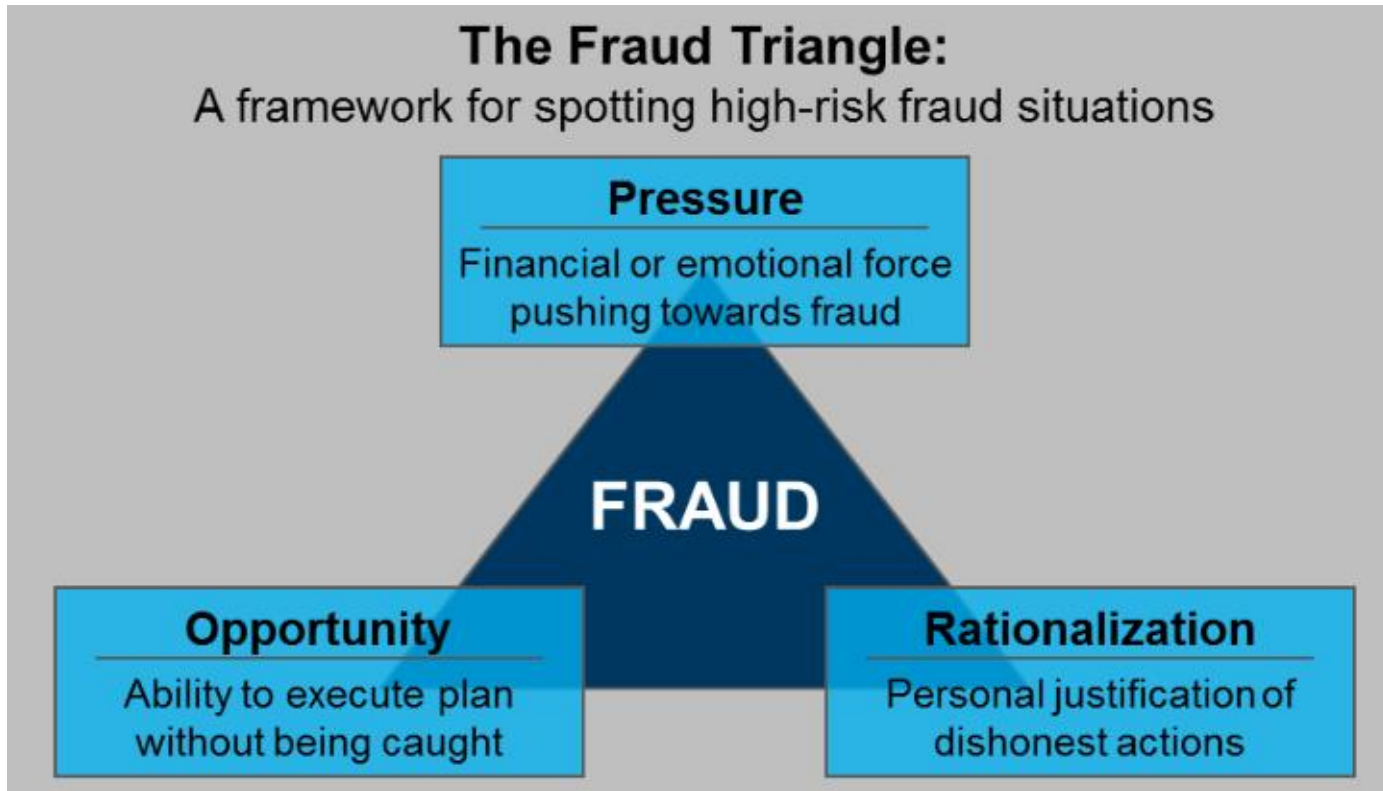
The fraud triangle originated from Donald Cressey's hypothesis:

Trusted persons become “trust violators” when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.

Donald R. Cressey, *Other People's Money* (Montclair: Patterson Smith, 1973)
p. 30.



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer (cont'd)



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer (cont'd)

- Fraud is not always small growing over time.
- Lack of staff training and commitment to accounting – ripe conditions for a “trust violator” to operator.



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer (cont'd)

- Example: AAMC (Association of American Medical Colleges) (information provided via internet search)
 - one of the largest in Washington metro area – administers the MCAT
 - victim of a fraud over an 8 year period by a “trusted long time employee” – according to the CEO.
 - Bank accounts opened in names similar to organization “Brookings Institution” NOT “Brookings Institute”.
 - Phony invoices in names of legitimate groups approved for payment with checks returned to perpetrator (not the vendor) and deposited into accounts perpetrator opened.
 - Employee was sole sign off for invoices up to \$20K.
 - Payments to what seem like a reliable organization – unchallenged.



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer (cont'd)

- Example: Virginia Scholastics Rowing Association (information provided via internet search)
 - Treasurer touted and lauded because she did the job gratis.
 - Treasurer entrusted with collecting, counting and depositing cash receipts and donations received at all the regattas.
 - Outside vendor sent email about 1 year old \$38,000 unpaid bill. Treasurer protested in tears it had been paid.
 - Secretary of organization went to bank to clear up and found over years, thousands spent on personal items by treasurer.
 - Association will never know exactly how much cash was lost.



I. Common and Clever Schemes Employees Use to Commit fraud Against Employer (cont'd)

- Example: American Legacy Foundation (information provided via internet search)
 - Managed hundreds of millions drawn from a government settlement with big tobacco.
 - Estimated \$3.4M loss linked to purchases from a business described sometimes as a computer supply firm and at others as a barbershop, and to an assistant vice president who now runs a video game emporium in Nigeria.
 - Legacy officials waited nearly three years after an initial warning before they called in investigators.

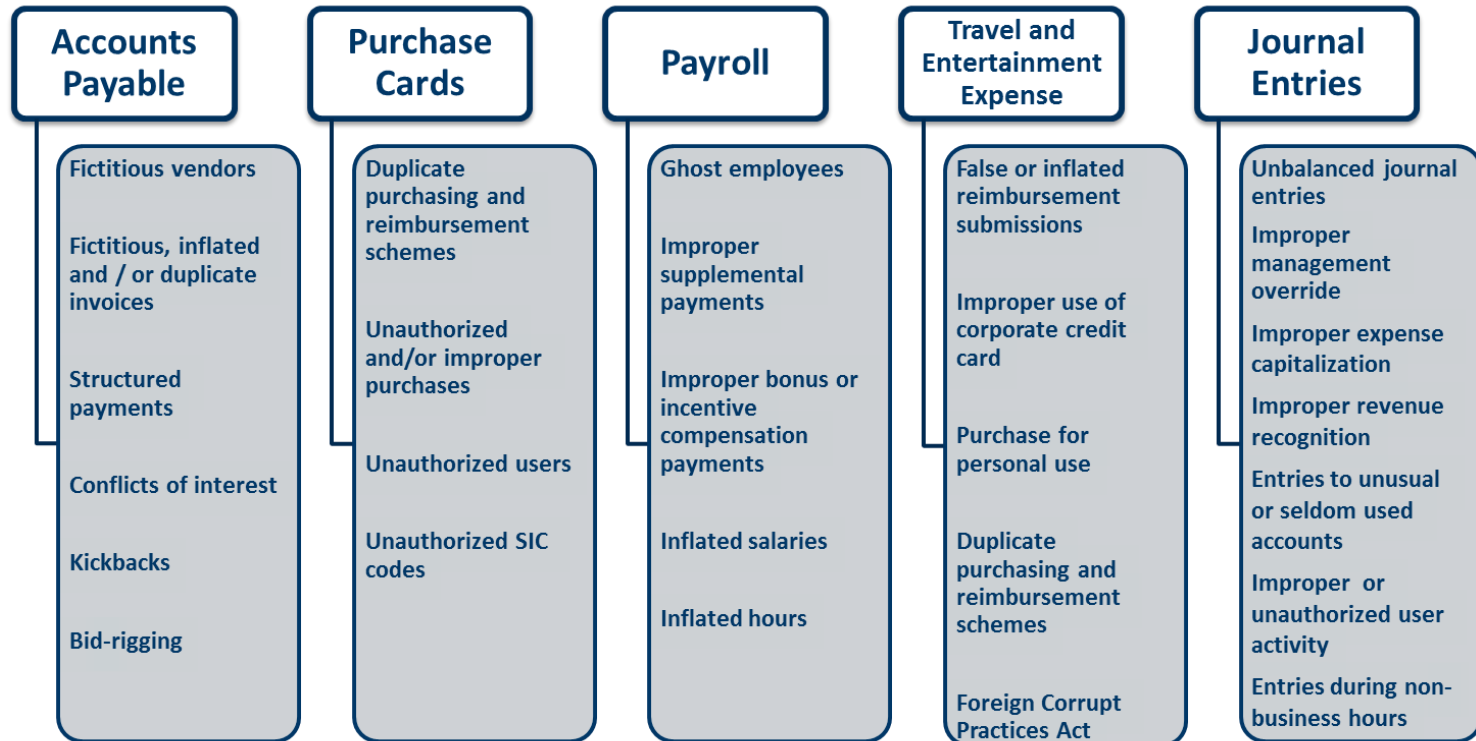


II. Warning Signs, Red Flags and Indicators of Predications of Theft or Abuse

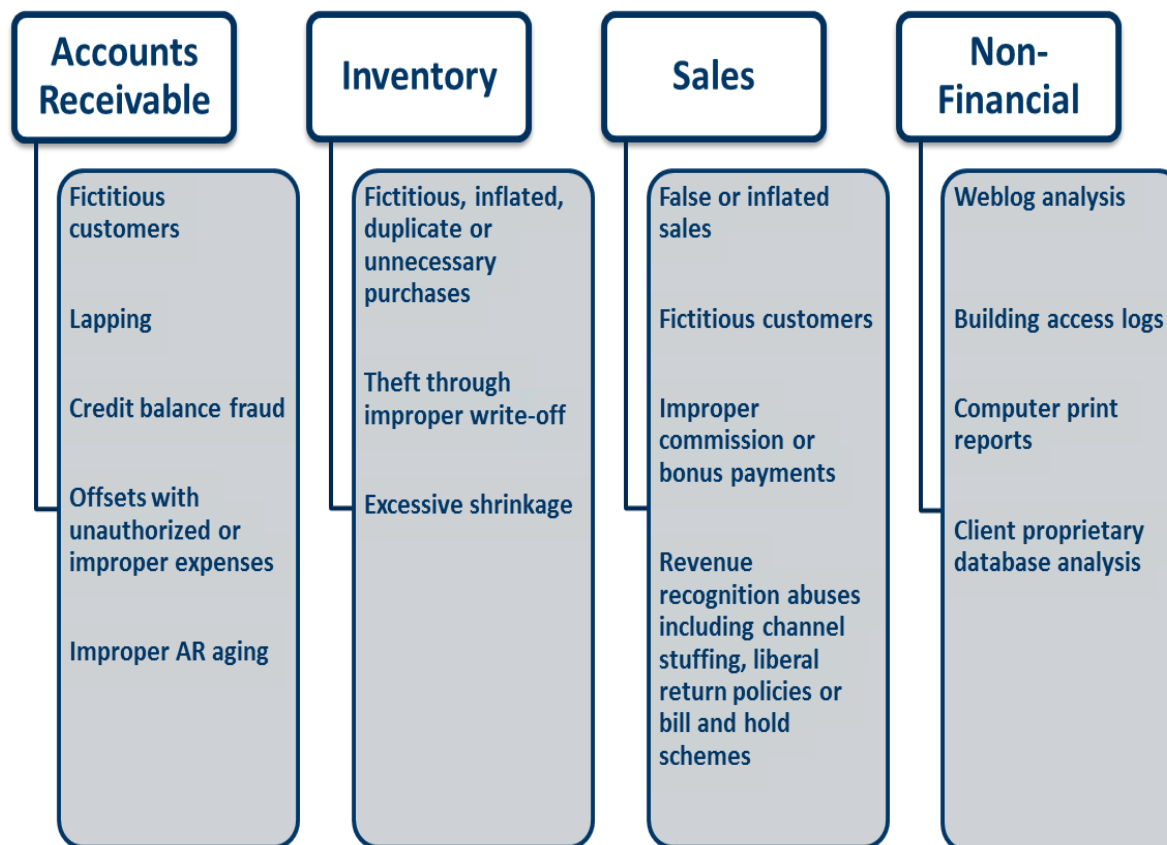
- Employees and other paid persons “living beyond their means”.
- Persons who DO NOT take vacation (credit card fraud and other misdeeds discovered this way).
- Significant diversions on 990s reported by more than 1,000 nonprofit organizations according to Washington Post article dated 10/26/13.



II. Warning Signs, Red Flags and Indicators of Predications of Theft or Abuse (cont'd)



II. Warning Signs, Red Flags and Indicators of Predications of Theft or Abuse (cont'd)



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized

Too Busy with the Programs and Wearing Blinders to What Goes Bump at Night – or Takes a Walk in Broad Daylight? Think About the following:

- Employee Handbook – document in writing with employees and executives signature and date that they reviewed, read, understood and agreed with the Employee Handbook.
- Bank account statements to CEO who should review for anomalies.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Review back of checks for subsequent endorsement.
- Hot line – effective only if in place and organization wide personnel are aware that management take the hot line seriously and follow up. Consider third party compliance reporting hot line.
- Closely review reimbursements to employees and company credit card statements.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Separation of duties – in smaller associations – consider Board members for some duties.
- Person processing invoices should only process for approved vendors.
- If a standard amount due monthly, set controls so that amounts larger cannot be processed without higher level approval.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Multiple reviewers for certain items – may seem ordinary but the “devil is in the details”. Example – corporate credit card reflected personal items, and seemingly business items – but used for personal benefit. No blanket credit card approval should exist.
- Tone at the top and tone from the bottom: establish environment of accountability, responsibility and stewardship.
- Double signatures – on expenses over a threshold.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Due diligence on vendors.
- Internal controls – not just something auditors look at – organizations need to own accountability and responsibility.
- Data analytics on key general ledger accounts (compare to bank documents)
 - Cash
 - Accounts Receivable
 - Accounts Payable



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Employee reimbursements from personal credit cards – keep to a minimum.
- Employee advances should be approved just as vendor invoices are approved.
- Process payment after services provided, if advance payment required, seek a deposit until service fully performed.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Contractors/consultants – should be independent of the organization. Approval documented if such person is not deemed independent but Association believes should be retained.
- Central supply – keep supplies guarded and locked. Examples include employees helping themselves by putting items in pockets, pocket books, baggy clothes, coats
- Travel advances and expense reports – are they approved?



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- KYC, KYE, and KYV (Know Your Customer – Know Your Employee and Know Your Vendor).
 - Clear Report on employees and key vendors.
 - Due diligence on vendors and approval documentation for period, amount.
 - Seek vendor certification that they are in compliance with FCPA and other requirements.
 - CHECK ALL deliveries to make sure what is ordered is received (personal items ordered at staples – does this make sense)? Person checking supplies in should be different than person ordering.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- No loans to employees, directors and related parties.
- Contracts should be reviewed and approved by the Board of Directors for key executives
- Risk assessments – perform periodically based on management/board assessment of the largest areas of concern – COSO Model (Committee of Sponsoring Organizations of the Treadway Commission) has five interrelated components.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

COSO Model:

Control Environment	<ol style="list-style-type: none"> 1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	<ol style="list-style-type: none"> 6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	<ol style="list-style-type: none"> 10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	<ol style="list-style-type: none"> 13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	<ol style="list-style-type: none"> 16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Recurring risk assessments – periodically select certain financial processes (different) and test to determine if policies and procedures are followed. Increase awareness of the periodic testing – acts as a deterrent.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.



III. Controls Aimed to Reduce Risk of Fraud and keep Reputational Risk Minimized (cont'd)

- Protect passwords
- OPM and OPA – Other Peoples Money and Other Peoples Assets.
- Don't forget to look at liabilities and expenses – often indicative of costs related to asset – but is the asset on the Association books?
- Budget to Actual review should be mandatory and at least quarterly.



IV. Recommendations to Consider when Suspicion of Fraud Exists

- Report to the Board of Directors, Audit Committee or other governing body as directed by the employee handbook. Reporting should be one level higher than the person involved.
- Board determines when to Retain Counsel, and which counsel to retain. Forensic accountant should be retained by the lawyer (with client paying the bill) – this protects “privilege” because you do not know what you do not know.



IV. Recommendations to Consider when Suspicion of Fraud Exists (cont'd)

- Retain forensic specialist to image computers immediately of persons under suspicion (can be done in evening).
- Notify insurance company
- Notify law enforcement
- Forensic Accountant (as consultant) can interview people to report to Management re “Platinum Practices”. Trained forensic people are accustomed to interviewing and can do so in a “non-threatening way”. Management often finds the interviewing distasteful and delegates to a consultant.



IV. Recommendations to Consider when Suspicion of Fraud Exists (cont'd)

- Forensic Account or management under direction of Forensic Account to calculate the loss.
- Plan the messaging re the event and communicate appropriately what happened, what is being done to instill better controls, and what is being done to FIX IT.
- AVOID the temptation to sweep under the rug what happened. If unresolved, rumors and speculation result which can damage the Association.



IV. Recommendations to Consider when Suspicion of Fraud Exists (cont'd)

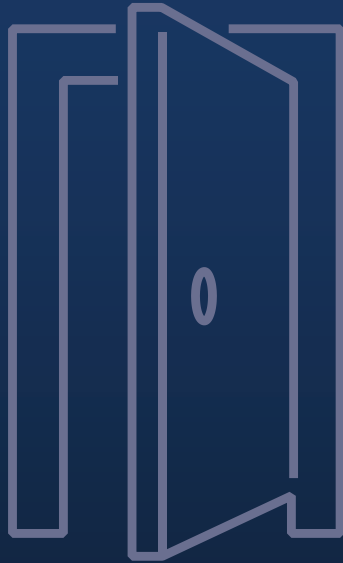
- Swift investigation is best and can dispel rumors and negative press
- One last thought – use professional skepticism. Be wary of “trust violators”. President Reagan said it best, “Trust but verify.”

Interesting book to read:

Snakes in Suits by Robert D. Hare

QUESTIONS?





Marion A. Hecht, CPA, CFF, CFE, CIRA, MBA
Principal
CliftonLarsonAllen LLP
marion.hecht@claconnect.com
Direct: 571-227-9613
Cell: 202-701-3921

CLAconnect.com