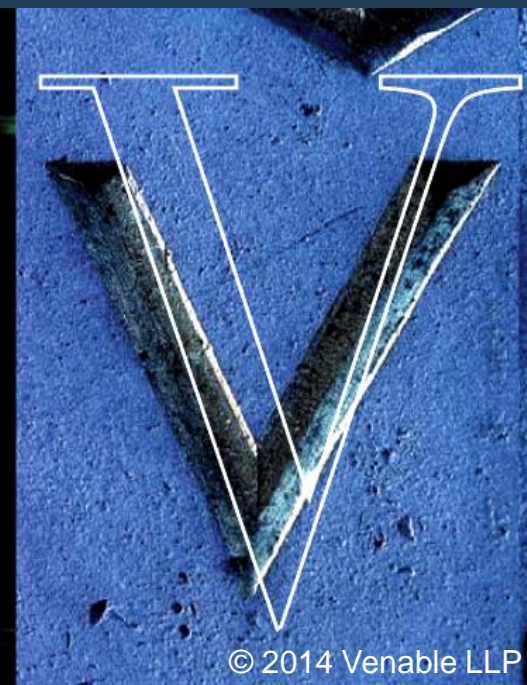
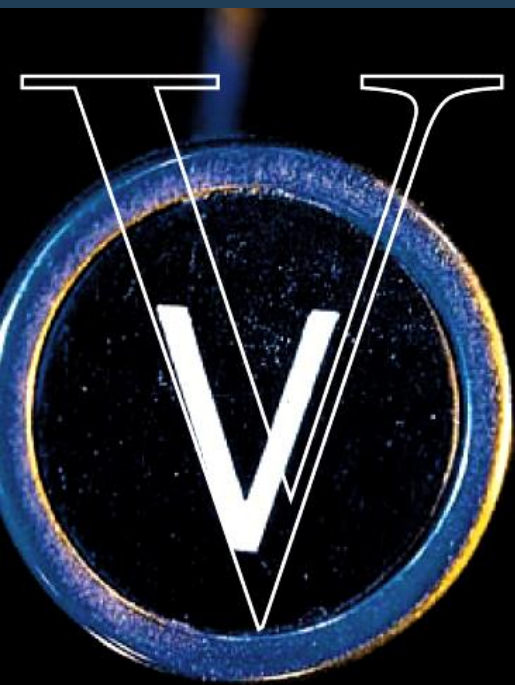


## *Second Annual Nonprofit Executive Summit:*

Bringing Nonprofit Leaders Together to Discuss Legal,  
Finance, Tax, and Operational Issues Impacting the Sector

Thursday, October 2, 2014  
Venable LLP  
Washington, DC





# Nonprofit Executive Summit Agenda

**Panel 1. Fraud and Embezzlement: The Executive Team's Role in Detecting, Reporting, and Preventing Fraud**

**Panel 2. Executive Employment Contracts: Getting Compliant and Creative**

**Keynote. Midterm Landscape 2014**

**Panel 3. Nonprofit Tax Issues: Where the IRS Is Today, and Where Congress Is Headed**

**Panel 4. Best Practices for Enhancing the Nonprofit Governance Model**



**PANEL 1**

**Fraud and Embezzlement:  
The Executive Team's Role in Detecting,  
Reporting, and Preventing Fraud**



*Moderator*



***Jeffrey S. Tenenbaum, Esq.***  
Partner  
Chair, Nonprofit Organizations Practice  
Venable LLP



***Mary Pat Flaherty***  
Investigative Reporter  
*The Washington Post*



***William H. Devaney, Esq.***  
Partner  
Co-Chair, FCPA & Anti-Corruption Group  
Venable LLP



***Marion A. Hecht, CPA***  
Principal  
Fraud & Forensic Investigations  
CliftonLarsonAllen







# Recent Examples of Nonprofit Fraud and Embezzlement





## Self, Inc.

- SELF, Inc. is a Philadelphia-based nonprofit organization that operates nine homeless shelters in the city.
- In August 2014, two former SELF executives were charged with theft stemming from allegations that they charged over \$350,000 to the organization's credit cards, spending the money on luxury items such as shoes and electronics, hotel stays and dining at the Four Seasons, and frequent trips to the Caribbean.
- Both former executives claim they reimbursed SELF, but prosecutors estimate they returned a pittance of what they spent (if they returned anything at all).
- The alleged embezzlement scheme began in 2005 and continued until 2010, just after both executives were fired.





# American Legacy Foundation

- In 2013, Sen. Charles Grassley (R-Iowa) opened an investigation into the American Legacy Foundation, a nonprofit dedicated to educating the public about the dangers of smoking.
- The investigation was spurred by a *Washington Post* report that the foundation had suffered an estimated \$3.4 million loss as a result of alleged embezzlement by a former IT specialist.
  - According to the *Washington Post*, the IT specialist generated 255 invoices for computer equipment sold to the foundation from 1999 to 2007, 75 percent of which were fraudulent.
  - When a whistleblower came forward (after his concerns were ignored years earlier), the foundation hired forensic examiners and notified the board of directors.
  - The U.S. Attorney's Office told the *Post* that its investigation had been closed in February 2012...***because the foundation had taken more than three years to report the missing equipment and lacked reliable records.***





# Vassar Brothers Medical Center

In late October 2013, the *Washington Post* reported that Vassar Brothers Medical Center in Poughkeepsie, New York, reported a 2011 loss of \$8.6 million through the "theft" of certain medical devices.

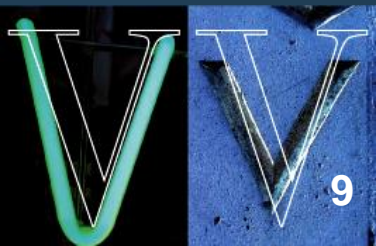






# American Red Cross (NY Chapter)

- On February 27, 2013, the former financial director for a New York chapter of the American Red Cross was sentenced to two to seven years in prison for grand larceny.
- As signatory to the chapter's operating account, the former director obtained an ATM debit card in her name and linked to the chapter's account to make cash withdrawals, sometimes as often as every few days.
- The former director used the money to pay for clothing, her children's tuition, and other personal expenses, embezzling over \$274,000 between 2005 and 2009.
- The missing funds were uncovered by an audit.





# H.O.W. Foundation

- On November 8, 2012, the former executive director of the H.O.W. Foundation, a nonprofit alcohol and drug treatment center in Tulsa, was sentenced to 15 months' imprisonment and ordered to pay over \$1.5 million in restitution for defrauding H.O.W. over the course of eight years.
- The former executive director wrote himself 213 unauthorized checks totaling over \$1.35 million. He also embezzled more than \$200,000 from a thrift store operated by the nonprofit.





# Global Fund to Fight AIDS, Tuberculosis and Malaria

- In 2012, the Global Fund to Fight Aids, Tuberculosis and Malaria, (based in Geneva) reported to the federal government a misuse of funds or unsubstantiated spending of \$43 million by grant recipients in several countries.
- In a 2013 report, The Global Fund determined that 1.9 percent of Global Fund grants were misspent, fraudulently misappropriated, or inadequately accounted for.

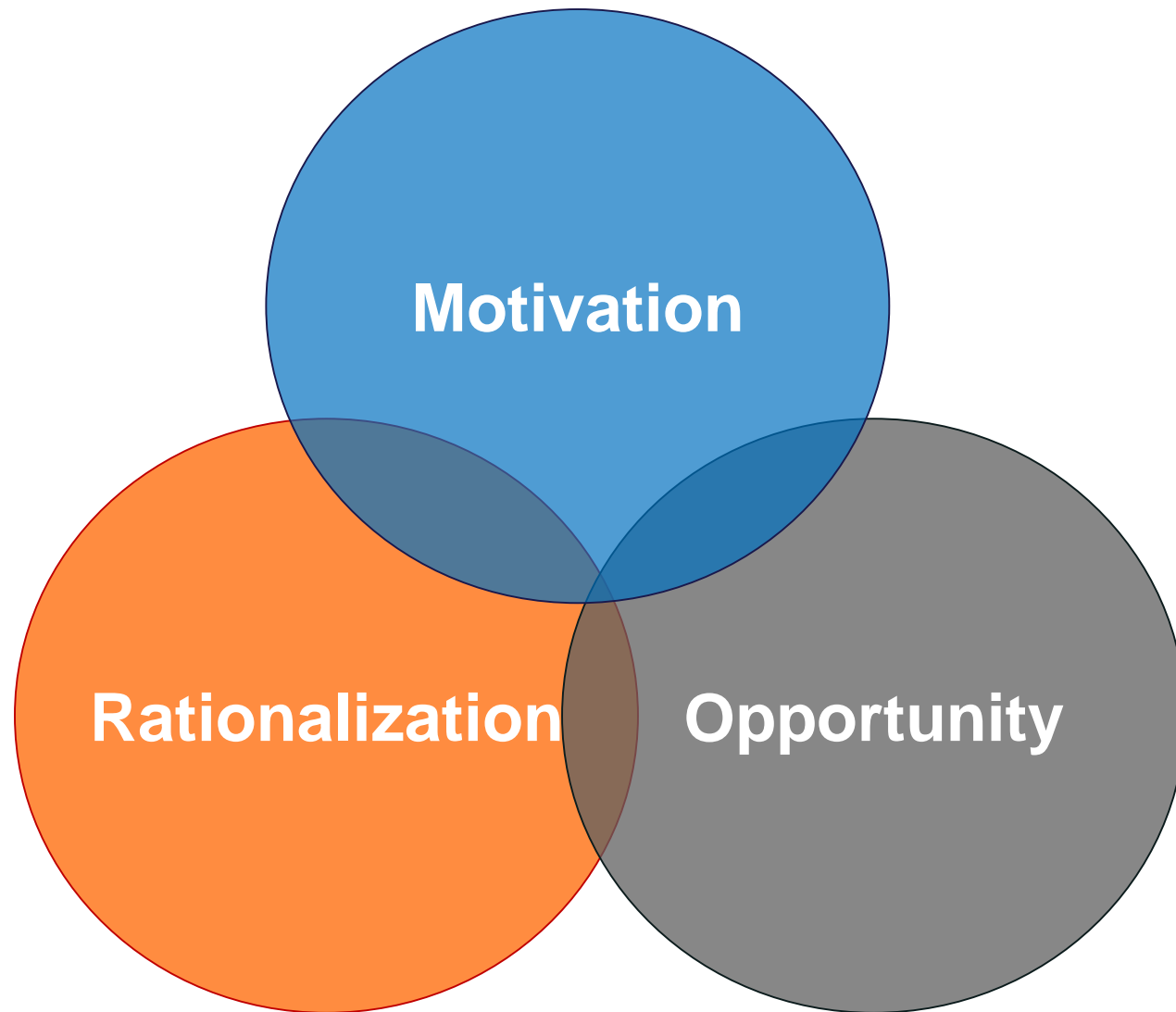




# Why Does Employee Fraud Occur?



# Why Does Employee Fraud Occur?







# Why Does Employee Fraud Occur?

## Motivation

Economic factors such as personal financial distress, substance abuse, gambling, overspending, or other similar addictive behaviors may provide motivation.

## Rationalization

The employee finds a way to rationalize the fraud...perceived injustice in compensation compared to for-profit enterprises, unhappiness over promotions, the idea that they are simply “borrowing” and fully intend to return the assets at a future date, or a belief that the organization doesn’t really need the assets and won’t even realize they are missing.

## Opportunity

The employee has sufficient access to assets and information to believe the fraud can be committed and successfully concealed.





# Why Are Nonprofits Frequently the Victims of Embezzlement?

**Management and board members are often more trusting**

**Fewer stringent financial controls for nonprofits**

**A belief that audits will catch any fraud**





# Controls to Reduce Risk of Fraud





# Set the Tone at the Top

**Management,  
including directors  
and officers, need to  
“set the tone at the top”**

---

**Management  
must set a good example  
for fair and honest business practices**





# Role of the Board

- Boards of directors have a fiduciary duty to ensure
  - Financial decisions are made soundly and legally
  - Individual directors and management always put the organization's financial and business interests ahead of personal financial and business interests
  - The board prudently manages the organization's assets in furtherance of the organization's stated purpose
  
- Business Judgment Rule protects actions taken by board members. However, those actions must be taken in good faith, with the degree of diligence, care, and skill that ordinary prudent people would exercise under similar circumstances.







# Role of the Board

- Satisfying these obligations requires hands-on oversight of management
  - Review financial and other business records
  - Question management
  - Ensure the organization's policies, procedures, and mission are followed
- At least one board member should have relevant financial experience
- At least some board members should not be current or former associates of management. Consider a seasoned lawyer as a board member, as well as members with nonprofit and sector expertise.





# Fraud Risk Assessments

- The purpose of a fraud risk assessment is to identify where fraud may occur within an organization and how it may be perpetrated.
- The assessment process:
  - Define fraud as it pertains to the organization's industry, culture, and tolerance for risk;
  - In collaboration with management and other appropriate employees, identify relevant fraud risks and scenarios
  - Organize fraud brainstorming sessions for selected processes and/or departments
  - Map fraud risks with their mitigating controls and identify control gaps;
  - Measure each fraud risk; and
  - Prioritize fraud risks
- Conduct such assessments on a recurring basis. Risk level/tolerance may change.





# Segregation of Duties

- One individual should not be responsible for an entire financial transaction
  - Record
  - Reconcile
  - Custody of assets
  - Authorization
- Money Coming In: No single individual should be responsible for receiving, depositing, recording, and reconciling the receipt of funds.
- Money Going Out: No single individual should be responsible for authorizing payments, disbursing funds, and reconciling bank statements.
- Not enough staff to segregate these duties? Utilize compensating controls.





# Double Signatures and Authorizations

- Multiple layers of approval make it far more difficult for embezzlers to steal from your organization.
- For expenditures over a pre-determined amount, require two signatures on every check and two authorizations on every cash disbursement.
- Consider having an officer or director be the second signatory or provide authorization for smaller organizations.
- For credit cards, require prior written approval for costs estimated to exceed a certain amount.
- The person using the credit card cannot be the same person approving its use.
- Have a board member or officer review the credit card statements and expense reports of the Executive Director, CFO, CEO, etc.





# Require Backup Documentation

- All check and cash disbursements must be accompanied by an invoice showing that the payment is justified.
- If possible, the invoices or disbursement requests should be authorized by a manager who will not be signing the check.
- Only pay from original invoices.







# Never Pre-Sign Checks

- Many nonprofits do this if the executive director is going on vacation.
- Keep blank checks and signature stamps locked up.





# Purchasing and Fixed Asset Controls

## ■ Fair Bidding Process

- All contracts over a pre-determined financial threshold should be subject to at least three bids, and approved by a manager uninvolved in the transaction.
- Large contracts should be reviewed and voted on by the board.
- Extensive review of related party transactions

## ■ Fixed Asset Inventories

- Conduct a fixed asset inventory review at least once per year to ensure that no equipment (computers, printers, etc.) is missing
- Record the serial numbers of the equipment and consider engraving an identifying mark on each item in case of theft





# Automated Controls

- Use system-generated reports to detect fraud when it occurs.
- Provide ongoing monitoring and feedback mechanisms (*e.g.*, system-generated e-mails notifying management of exceptions)
- Physical access codes
- System passwords
- Use notification and alert services to alert the organization of possible debits to accounts.
  - Positive pay exceptions notifications
  - Wire notifications (incoming/outgoing)
  - ACH Fraud Filter notifications
  - Balance threshold notifications





# Conduct Background Checks

- Background checks on new employees and volunteers are important. Many organizations skip this basic step.
- The Association of Certified Fraud Examiners reports that 7% of embezzlers have been convicted of a previous crime.
- Background checks can reveal undisclosed criminal records and prior instances of fraud, allowing you to avoid a bad hire in the first place.
- They are also fairly inexpensive and should be made a part of your hiring process.





# Mechanisms for Reporting and Investigating Fraud

- Explain what to do if employees/constituents perceive a fraud threat.
  - Whom to contact
  - How to contact
  - Anonymity
  - Evaluations of reports received
  - Incident responses
- Provide a means of anonymous communication.
- Employees must have the means to contact a board member if something needs to be reported and they do not feel comfortable reporting to management.
- Board members must be prepared to take these reports seriously, keep the reporting employee protected, and contact legal counsel.







# Effective Compliance Programs

- The best way to prevent embezzlement and to protect an organization is a comprehensive and vigorous compliance program that is more than a mere “paper program.”
- Any effective compliance program will:
  1. Be tailored to the specific organization, so that the controls mitigate the risks inherent in that organization’s business and address any applicable government regulations and industry standards
  2. Include a written corporate code of ethics. The organization’s commitment to ethical behavior should be clearly and concisely communicated to the board, management, and employees. This commitment to the code should be affirmed by all employees on a periodic and ongoing basis.
  3. Be owned by senior management. Management must be proactive. The board must have ultimate oversight and control of the program.
  4. Provide for regular education and training for directors, management, employees, volunteers and staff





# Effective Compliance Programs

- Any effective compliance program will (cont'd):
  5. Be regularly monitored and audited to ensure that it is working
  6. Contain effective means to report violations and concerns, such as whistleblower hotlines or other anonymous reporting mechanisms
  7. Provide meaningful discipline for violation of the policy. A reputation for aggressively investigating fraud can have a strong deterrent effect, while a reputation for ignoring possible fraud is an invitation to commit fraud.
  8. Require that appropriate steps are taken if a crime occurs
  9. Address any control weaknesses uncovered





# What to Do if an Issue Is Discovered

- Selection of investigative team
- Evidence preservation
- Evidence gathering
- Background checks in an investigation
- Interviews
- Reporting
- Remediation





# Nonprofit Fraud...Exposed

FORM 990, PART VI, SECTION A, LINE 5: REGRETTABLY IN LATE APRIL  
 WAS DISCOVERED THAT A CSAVR EMPLOYEE HAD ENGAGED IN SIGNIFICANT  
 OF EMBEZZLEMENT AND EMPLOYEE THEFT FROM 2003 UNTIL APRIL 2010  
 DETERMINED THAT THE SAID EMPLOYEE ALLEGEDLY STOLE OVER \$824  
 CSAVR.

(Image courtesy of the *Washington Post*)



# Reputational Risk – Best Practices





# Things to Think About

## ■ Professional skepticism

- It is ok to ask questions to determine responses that do not make sense.
- Follow up and seek documentation and/or other supporting information.
- Rule of Two – Always a good idea to run questionable events or transactions by someone.
- Independent consultation is valuable.

## ■ Ostrich attitude

- Head in the sand – Can hurt the organization's reputation, sustainability, and economic stability.
- Instead – Four "I"s: Interview, Intervene, Interpret, Inspect....

## ■ Pressures

- Environment, Economic, Financial, Personal, Organization
- (Fraud Triangle – Rationalization, Pressure, Opportunity)





# Things to Think About

- Do you know where your assets are? What about liabilities?
- Big check?
  - Slow down and look beyond the numbers on the check to the issuer.
  - Gifts for no consideration can be “clawed back”.
  - Seek financial information on the donor, look at the footnotes to financial statements.
  - Ask questions.
  - Examples of damages to nonprofits
    - Ponzi schemer gifts that a Receiver will claw back.
    - Bankruptcy Code provides for preference actions against recipients of gifts based on facts and circumstances.
- Entity level controls
  - Employee handbook and code of conduct, regularly reviewed by all employees with signature/date.
  - Anti-fraud controls.







# Preventive Measures and Quick Tips

- Look at checks (front and back)
  - [Checks endorsed to subsequent payee]
  
- Bank statements should be sent to CEO, accounts reconciled on regular basis
  - [Payees altered and ATM withdrawals not authorized at strange times in the late evening]





# Preventive Measures and Quick Tips

## ■ Credit card abuse

- Look at the transactions and the purpose of the charges, and determine who has authorization to use the credit cards.
- Personal expenses NEVER should be charged on a corporate credit card.
- Document authority.
- Reimbursement from an employee – why not add --the requested reimbursement is pursuant to our firm policy and is true and complete.
- Seek advice from HR and potentially counsel before changing firm forms.
- [Senior executive used company credit card for personal use, travel for relatives, payments to consultants with less than arm's length relationship, additional credit cards paid by firm, among others.]
- [Look at contracts with board.]





# Internal Controls

## ■ Vendors

- Phantom or real? Or, related parties?
- Do employees have second jobs?
- Document and look at the possibility of organization funds used for purposes other than the allowed business purpose.
- [Classic examples include staff as well as management feeling they can rationalize the theft of firm assets for their off duty jobs, among other reasons.]

## ■ Process controls

- Over recording transactions, segregation of duties, approval limits, continuous monitoring, etc.





# Reminder – The Fraud Triangle

- Incentives and pressures
  - What are the incentives and pressures that drive financial performance?
- Opportunities
  - How strong are internal controls, internal audit department, and anonymous reporting programs?
- Rationalization/concealment
  - Character, ethical values, integrity, and how management may justify their actions





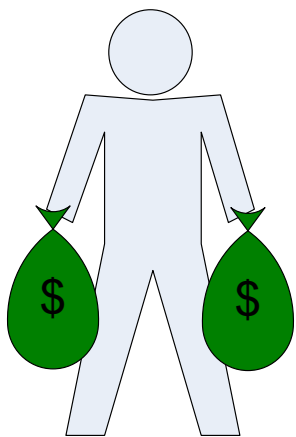
## Reminder - Fraud is defined as:

*“...any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain.”*

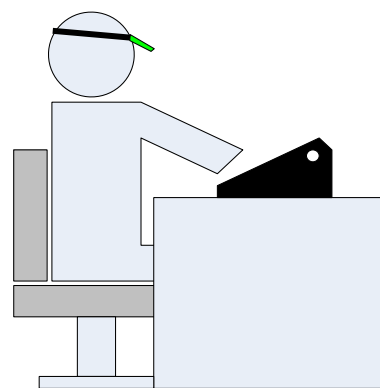
Source: *Managing the Business Risk of Fraud: A Practical Guide*



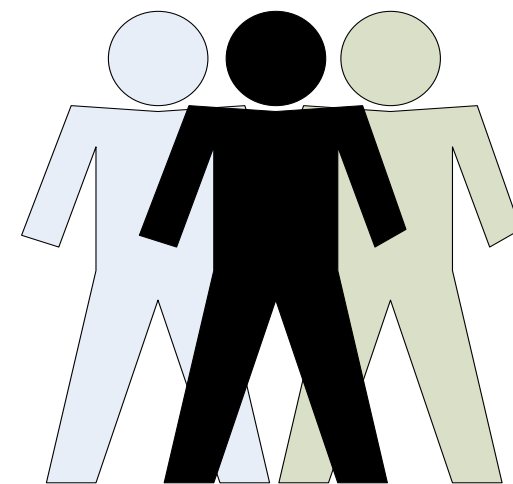
# Reminder – Three Fraud Categories



**Asset  
Misappropriation**

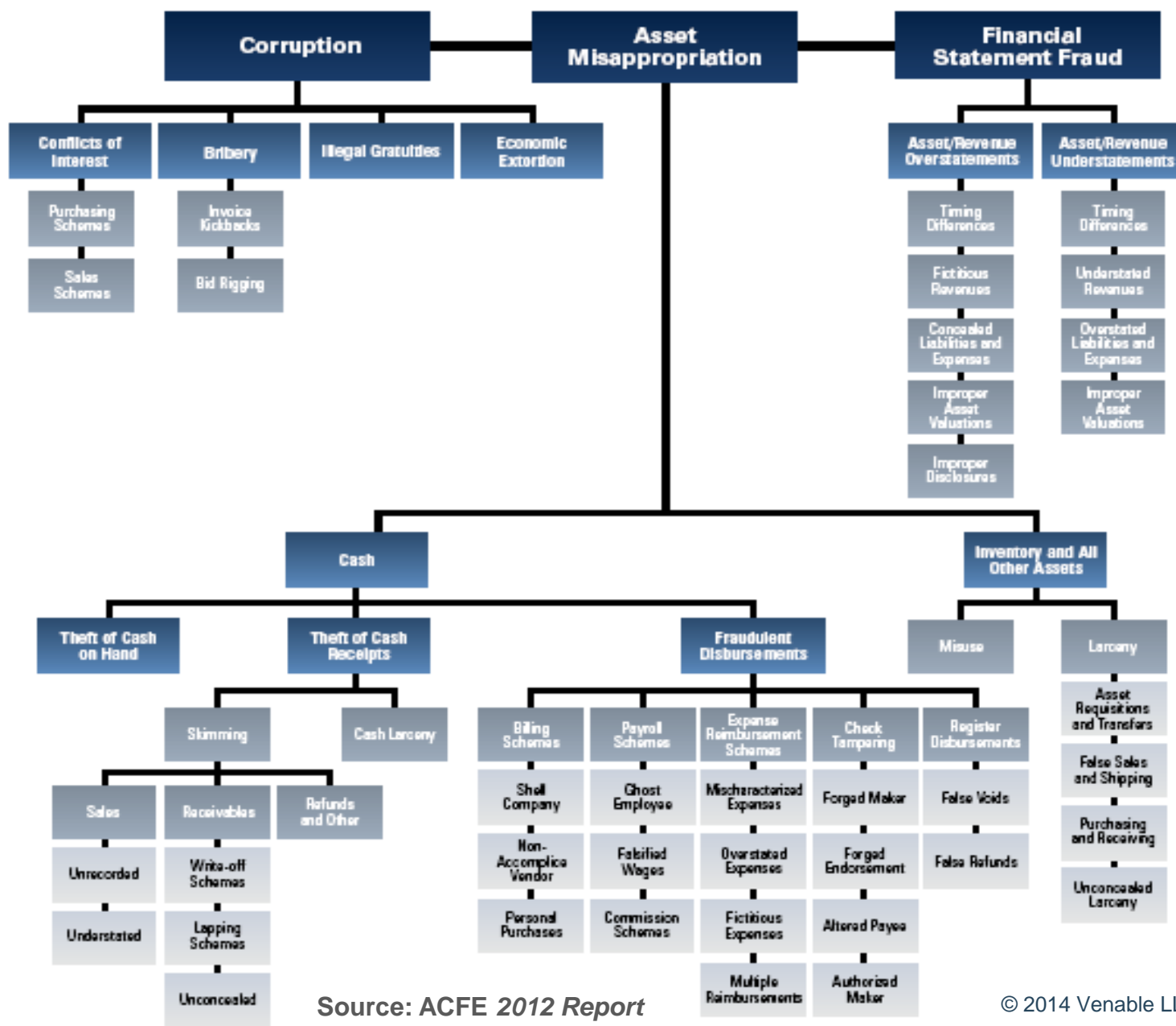


**Financial  
Statement Fraud**



**Corruption**

# Uniform Occupational Fraud Classification System



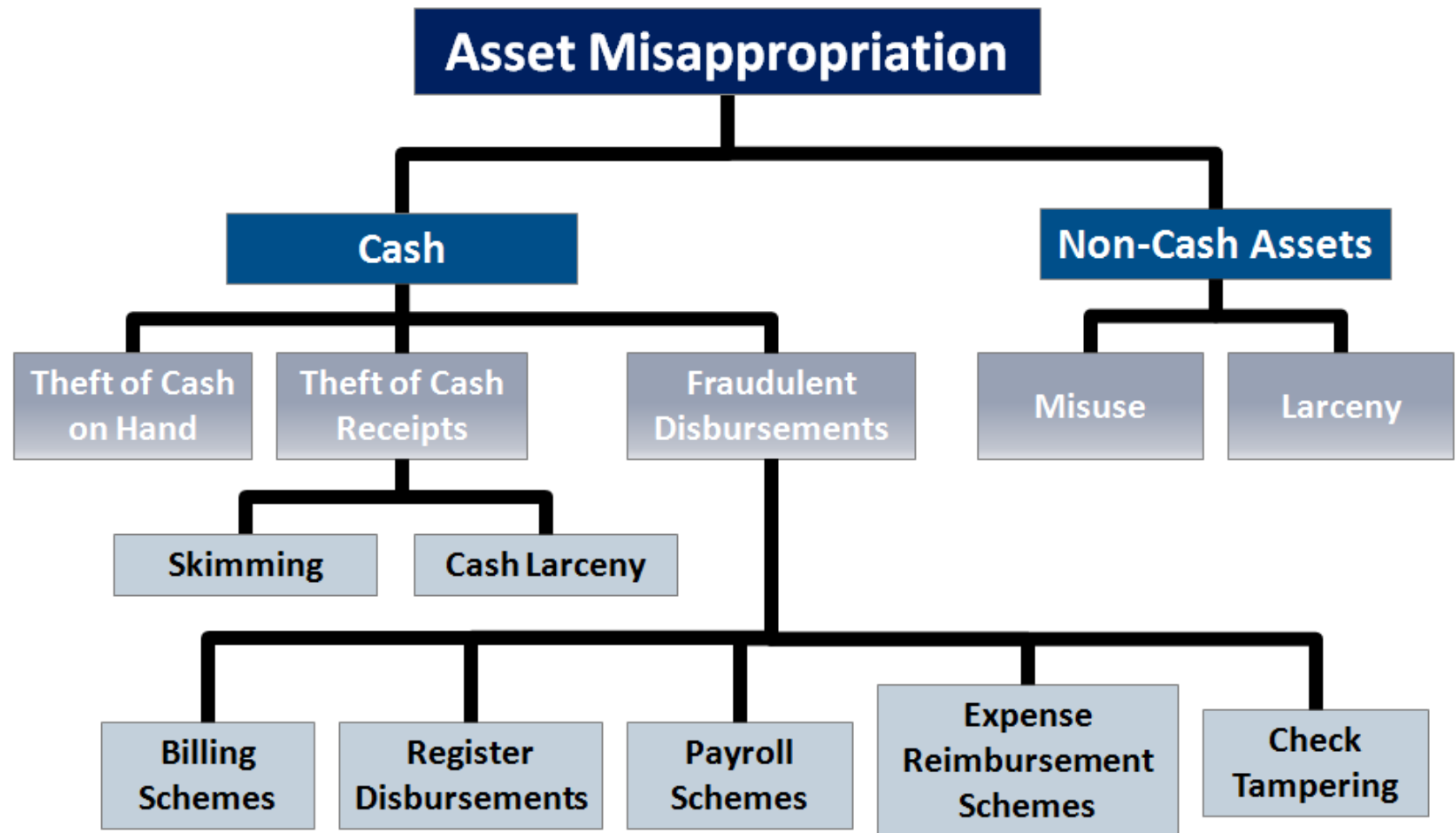
Source: ACFE 2012 Report  
to the Nations

© 2014 Venable LLP

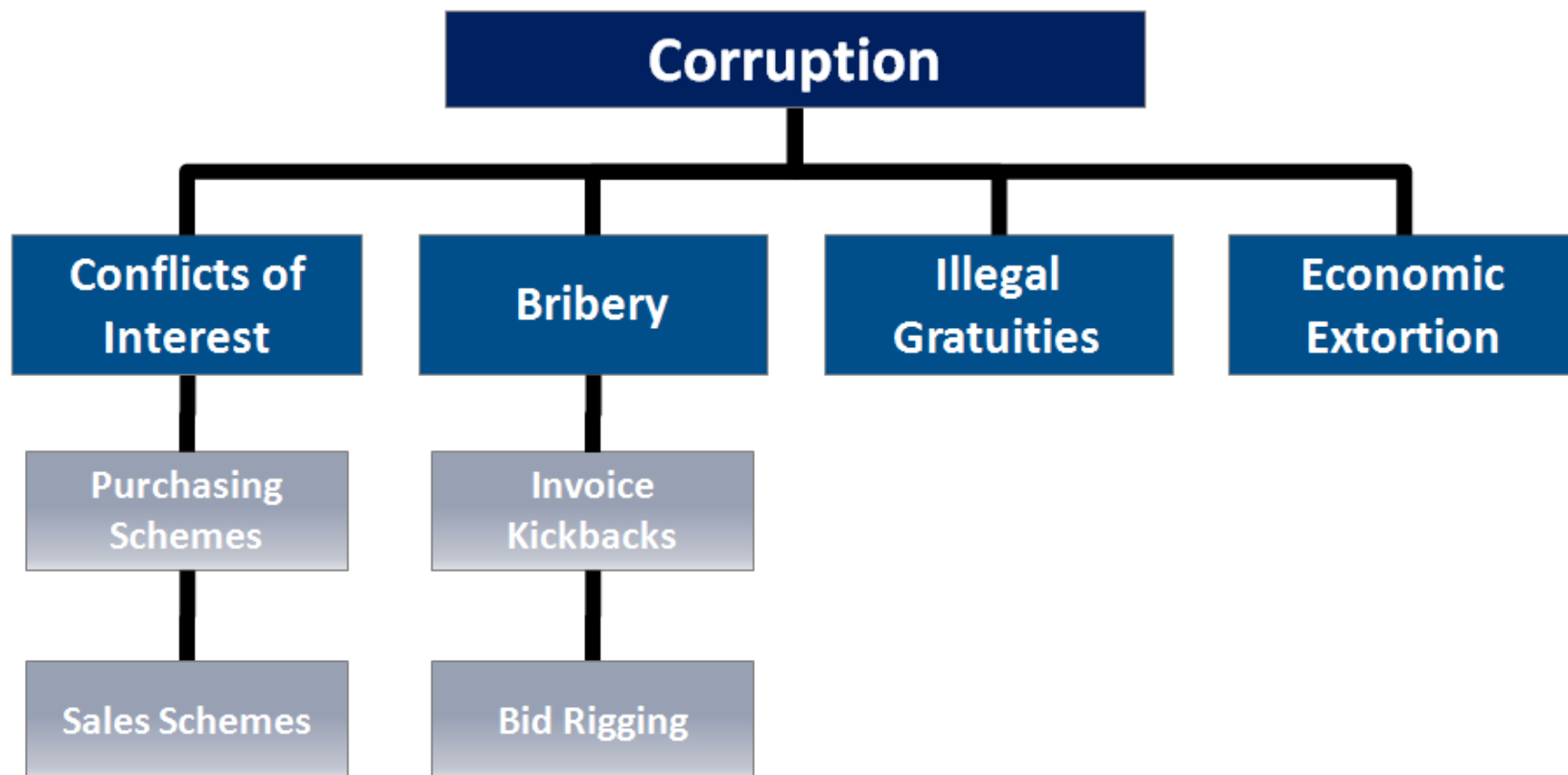




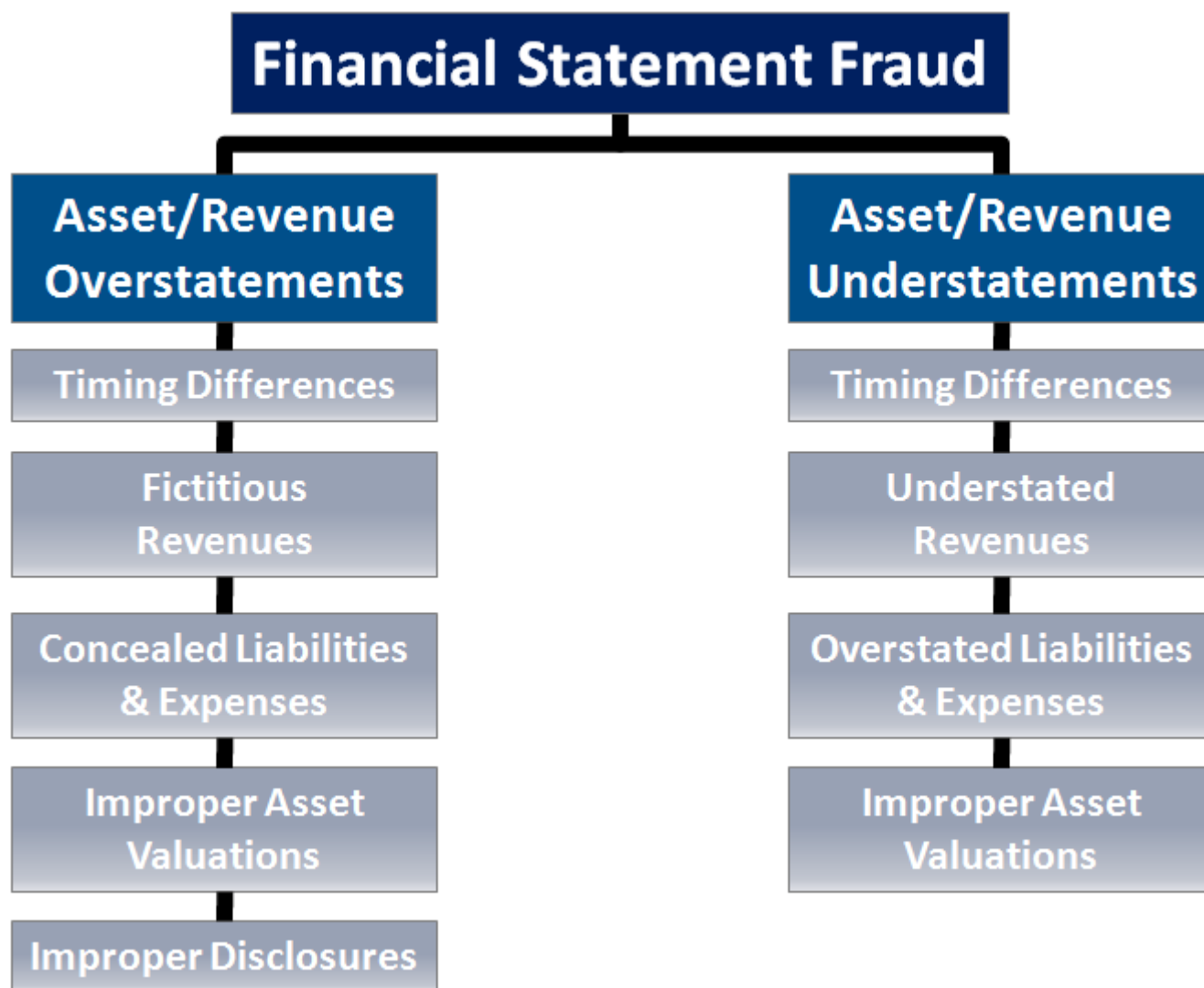
# Asset Misappropriation



# Corruption



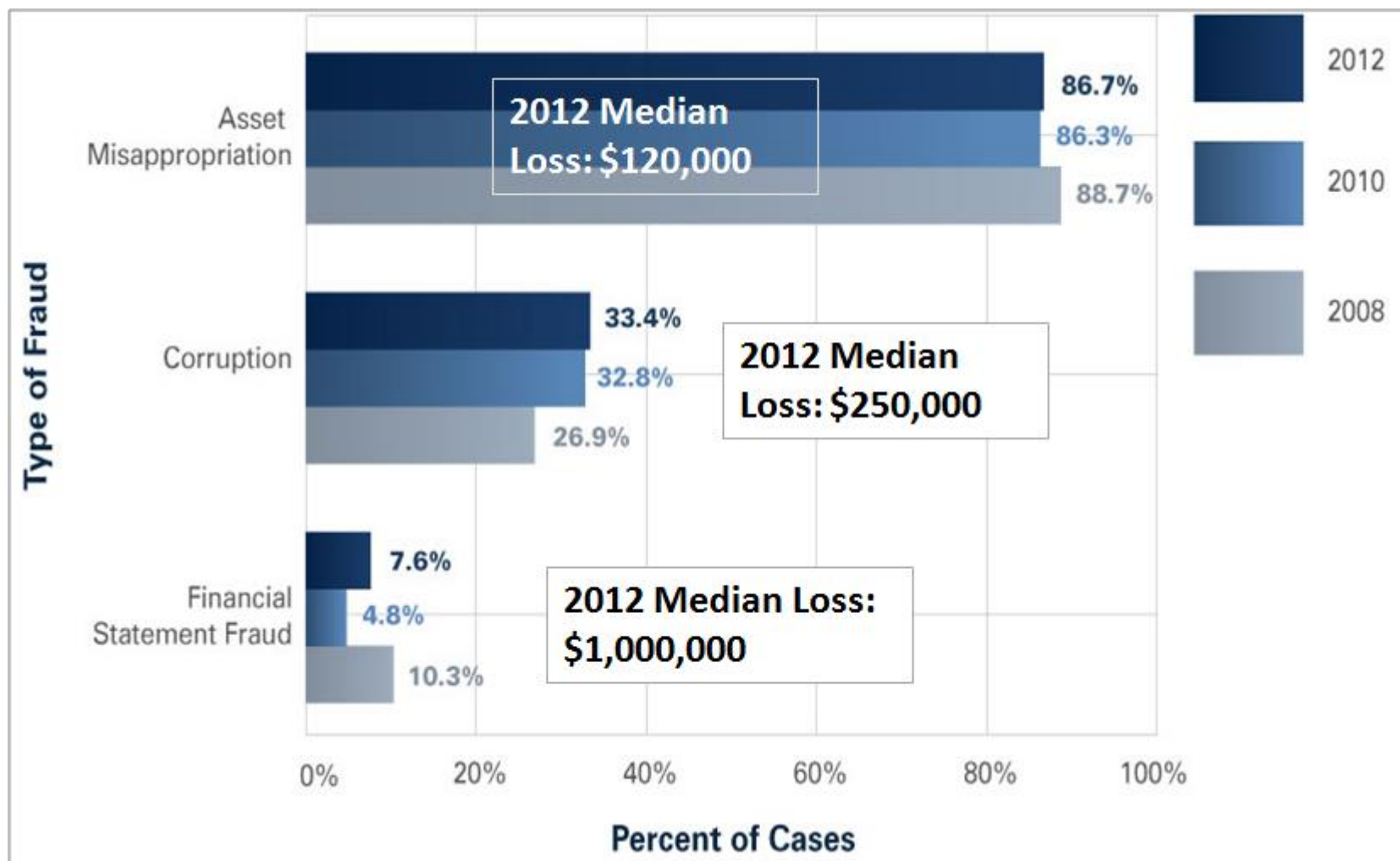
# Financial Statement Fraud





# Categories of Fraud

## Frequency of Fraud by Type



# How Fraud Affects Our Clients

- According to the ACFE's 2012 *Report to the Nations on Occupational Fraud and Abuse*:

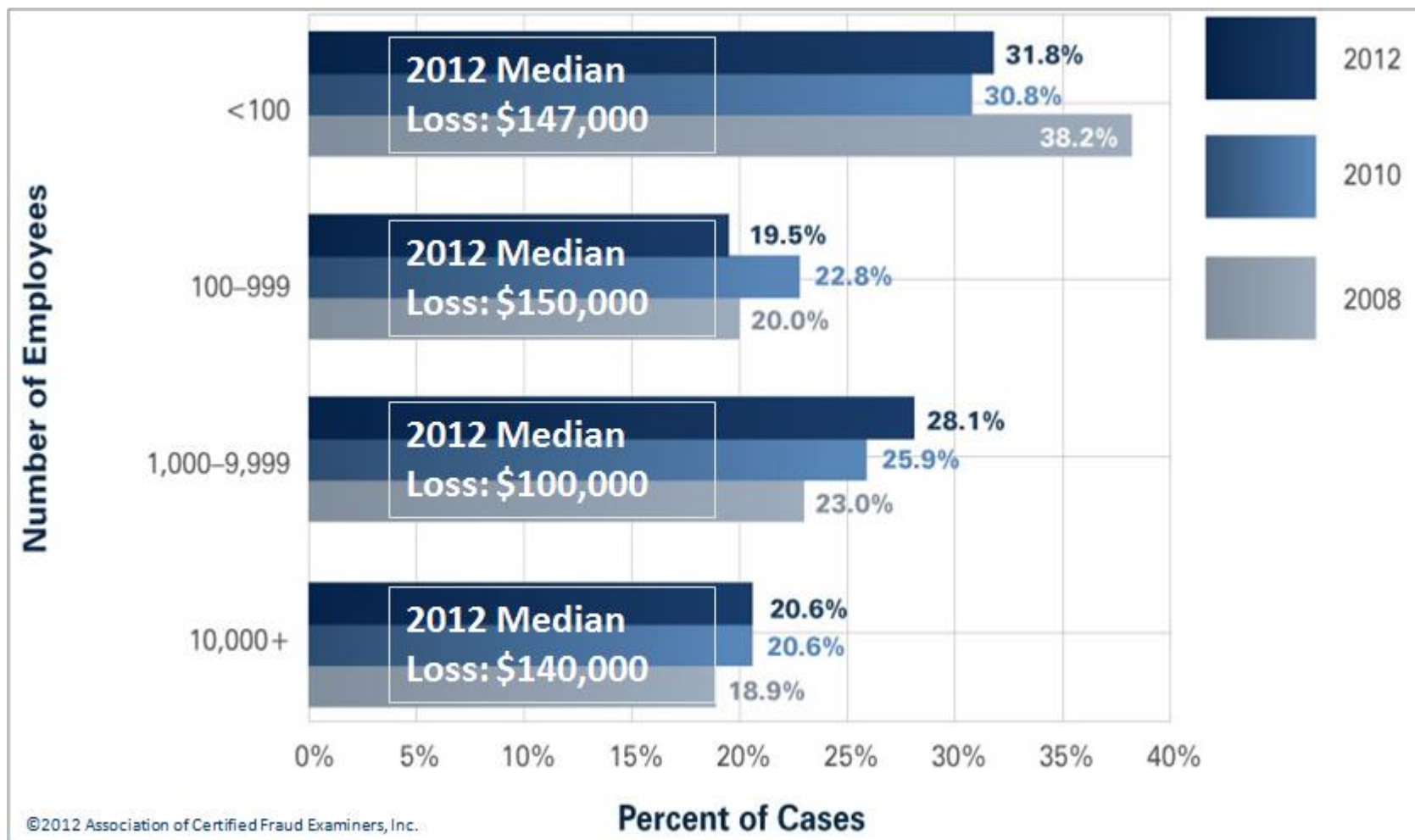


**The typical organization loses an estimated 5% of its annual revenues to occupational fraud.**

- Median loss: \$140,000
- Median duration: 18 mo.

# Victim Organizations

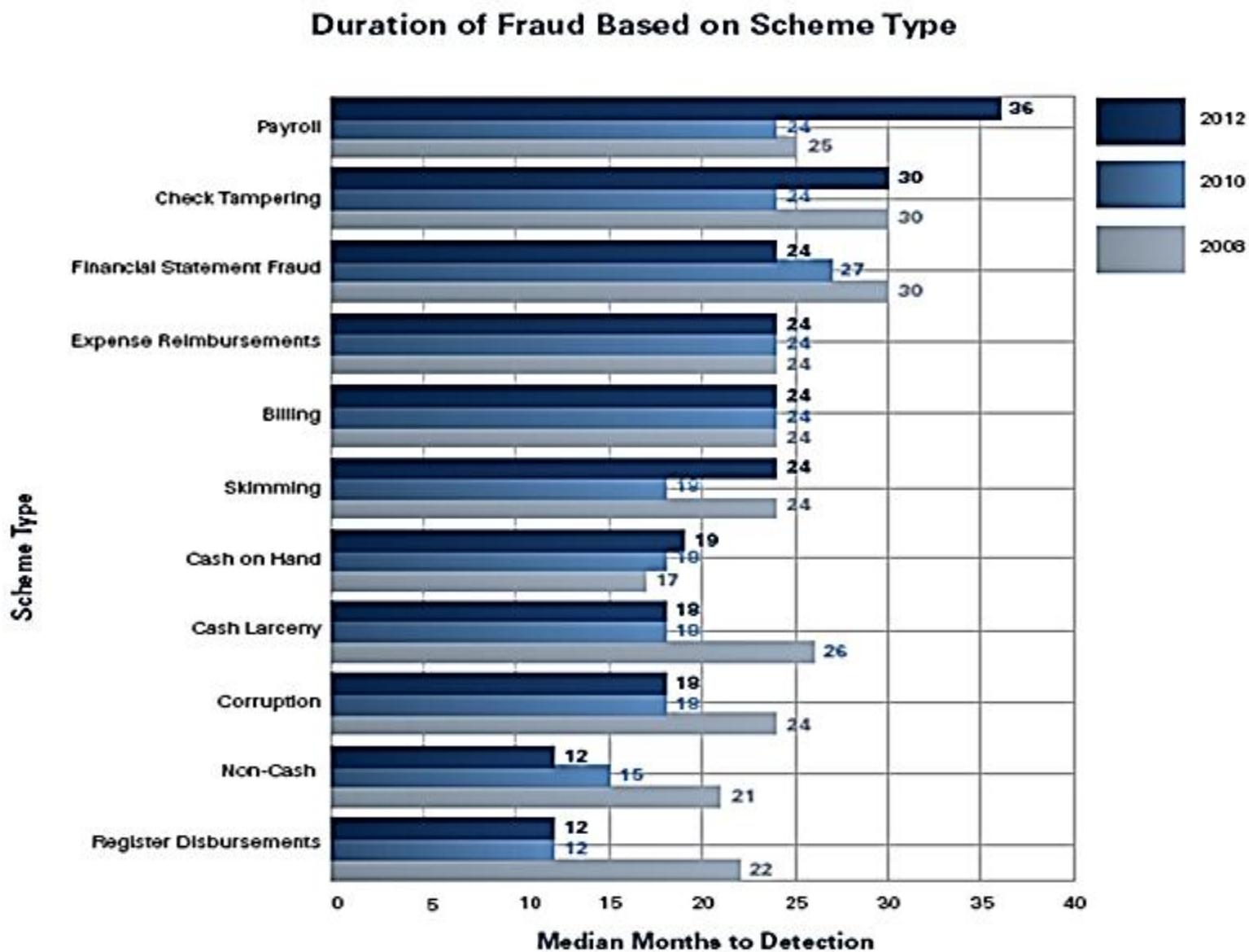
## Prevalence by Size of Victim Organization







# Gestation Period for Fraud Detection



Source: ACFE 2012 Report to the Nations





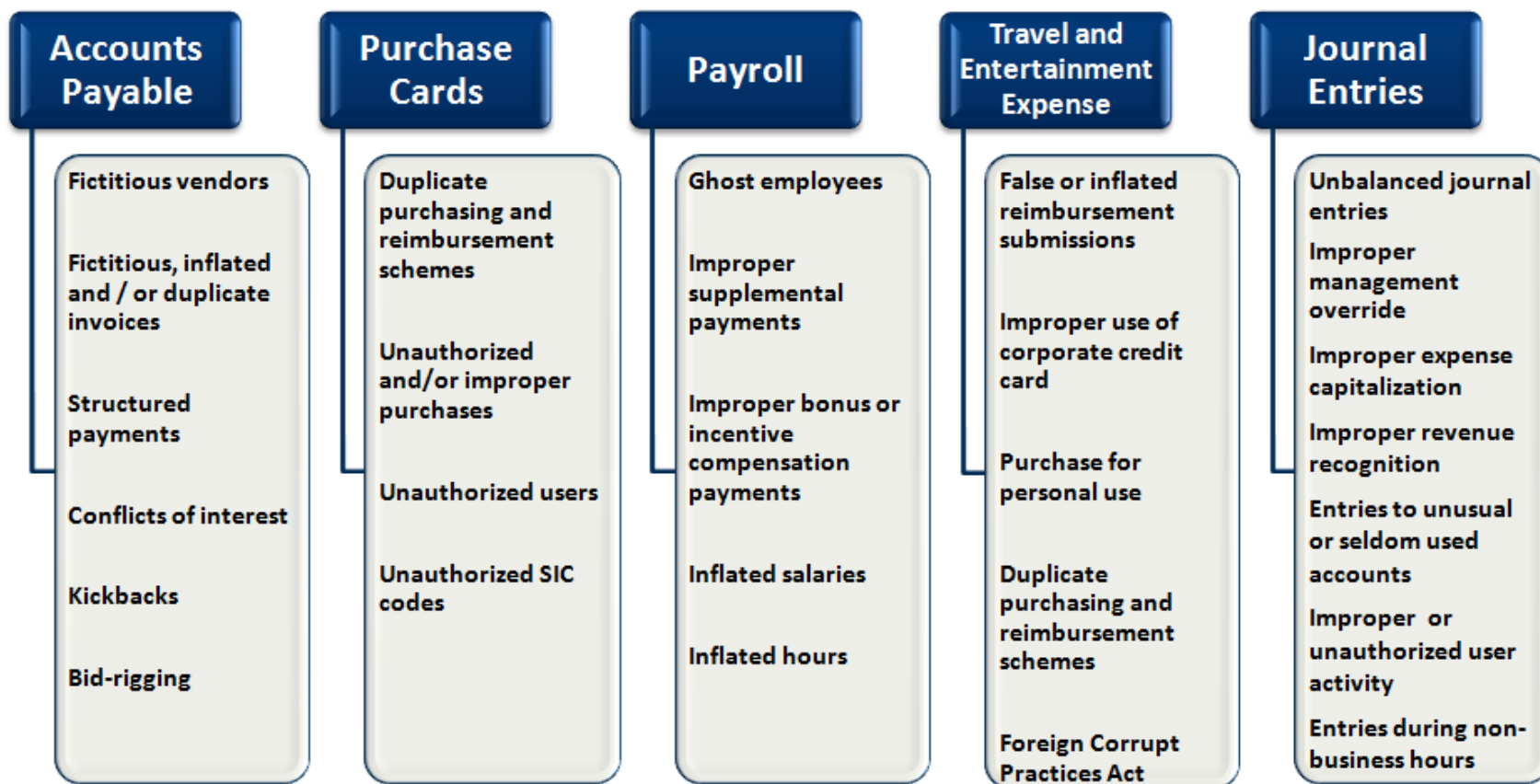
# Forensic Data Analysis

- **Forensic Data Analysis** is the process of gathering, summarizing, comparing, and aggregating existing disparate sets of data that organizations routinely collect in the normal course of business with the goal of detecting anomalies that are traditionally indicative of fraud or other misconduct.
- Can be used in the **prevention, detection, or response** of fraud or other misconduct
- Provides additional comfort to C-Level executives, audit committees, internal audit departments, and management



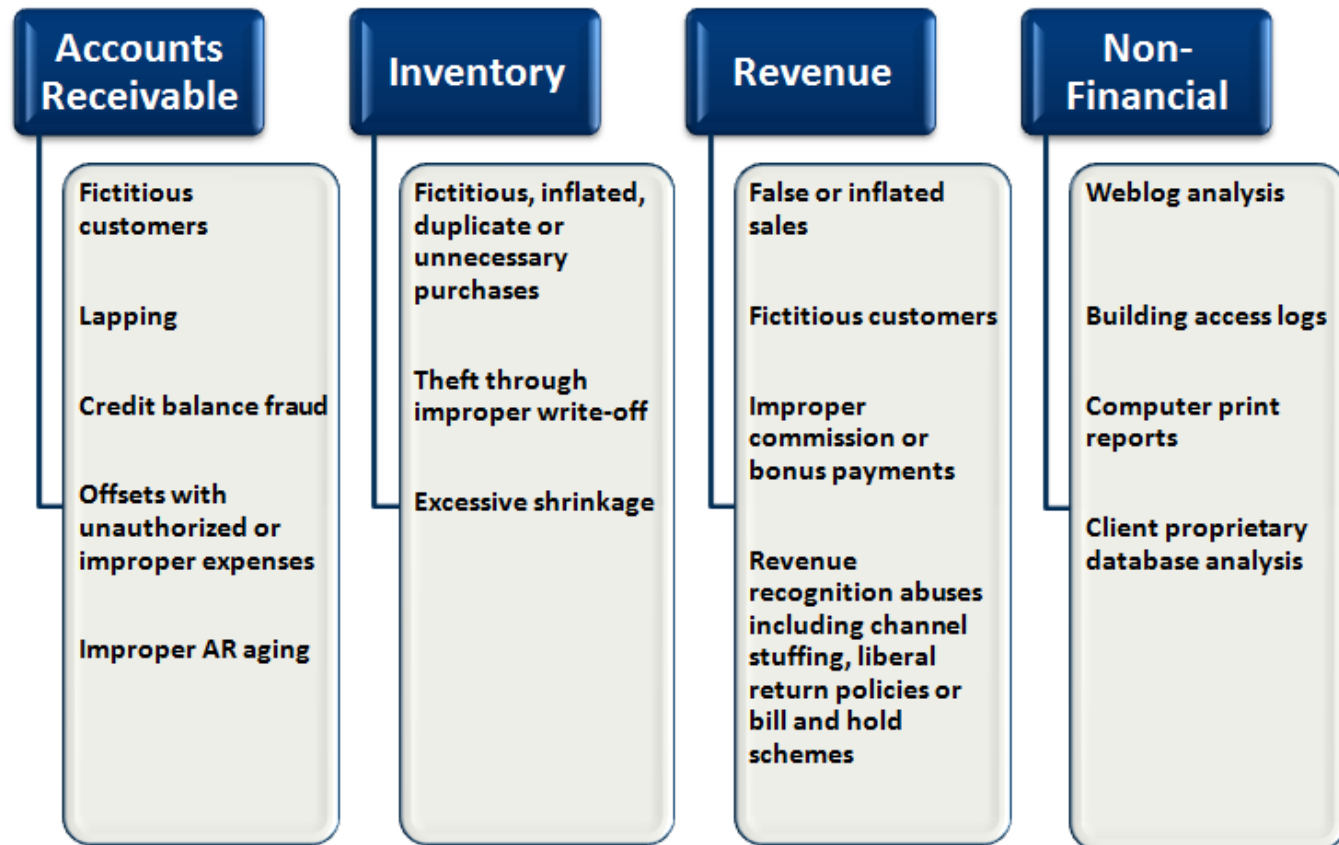


# Types of Fraud and Areas of Analysis





# Types of Fraud and Areas of Analysis





# Questions?





# Contact Information

**Jeffrey S. Tenenbaum, Esq.**  
**Partner and Chair of the Nonprofit Organizations Practice**  
**Venable LLP**

[jstenenbaum@Venable.com](mailto:jstenenbaum@Venable.com)

t 202.344.8138

**Mary Pat Flaherty**  
**Investigative Reporter**  
***The Washington Post***

d 202.334.7322

m 202.509.6395

@marypatflaherty

**William H. Devaney, Esq.**  
**Partner and Co-Chair of the FCPA and Anti-Corruption Group**  
**Venable LLP**

[whdevaney@Venable.com](mailto:whdevaney@Venable.com)

t 221.983.8204

**Marion A. Hecht, CPA, CFF, CFE, CIRA, MBA**  
**Principal, Fraud and Forensic Investigations**  
**CliftonLarsonAllen LLP**

[Marion.Hecht@CLAconnect.com](mailto:Marion.Hecht@CLAconnect.com)

t 221.983.8204



# Upcoming Venable Nonprofit Legal Events



# Upcoming Venable Nonprofit Events

## Register Now

October 21, 2014 – [Fundraising 201: An Update on Managing the Legal Risks of Nonprofit Fundraising](#)

November 19, 2014 – [Enhancing the Nonprofit Governance Model: Legal Pitfalls and Best Practices](#)

December 11, 2014 – [LGBT, Religion, and Diversity in the Nonprofit Workplace](#)





# Thank You!

**Jeffrey S. Tenenbaum, Esq.**  
**Partner and Chair of the Nonprofit Organizations Practice**  
**Venable LLP**

[JSTenenbaum@Venable.com](mailto:JSTenenbaum@Venable.com)

t 202.344.8138

**John P. Langan, CPA**  
**Managing Partner, Public Sector Group**  
**CliftonLarsonAllen LLP**

[John.Langan@CLAconnect.com](mailto:John.Langan@CLAconnect.com)

t 703.403.8296

To view an index of Venable's articles and presentations or upcoming seminars on nonprofit legal topics, see

[www.Venable.com/nonprofits/publications](http://www.Venable.com/nonprofits/publications) or  
[www.Venable.com/nonprofits/events](http://www.Venable.com/nonprofits/events).

To view recordings of Venable's nonprofit programs on our YouTube channel, see [www.youtube.com/user/VenableNonprofits](http://www.youtube.com/user/VenableNonprofits).

