

How to Safeguard Your Nonprofit against Fraud and Embezzlement: Best Practices, Common Pitfalls, and Practical Strategies

Wednesday, January 15, 2014, 12:30 p.m. – 2:00 p.m. ET

Venable LLP, Washington, DC

Moderator:

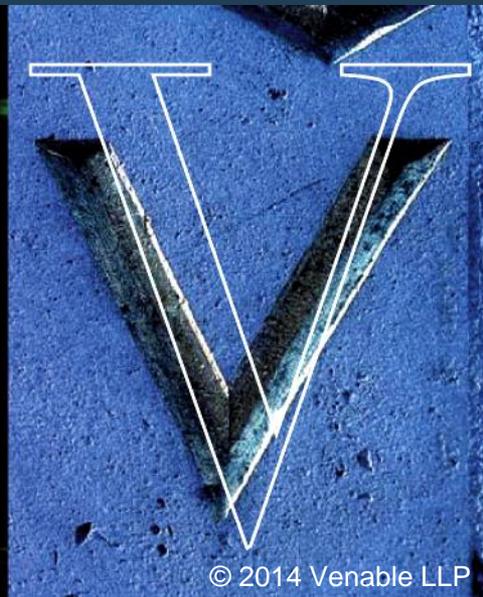
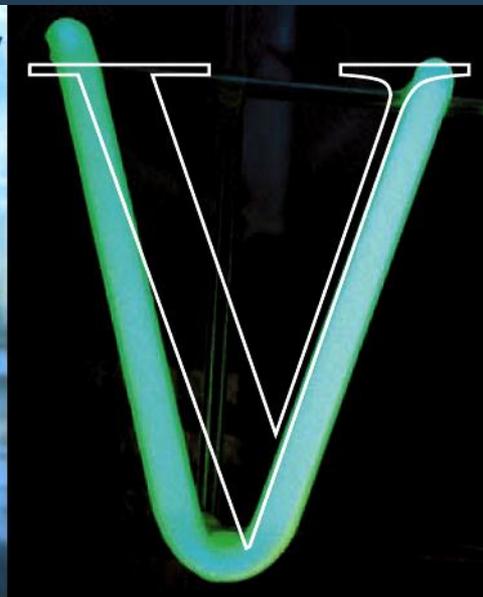
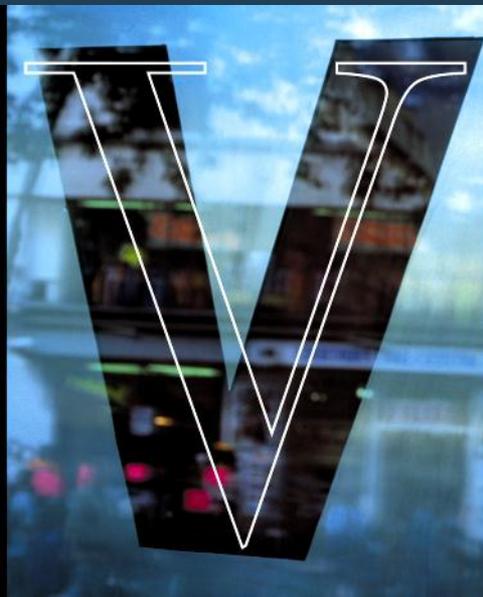
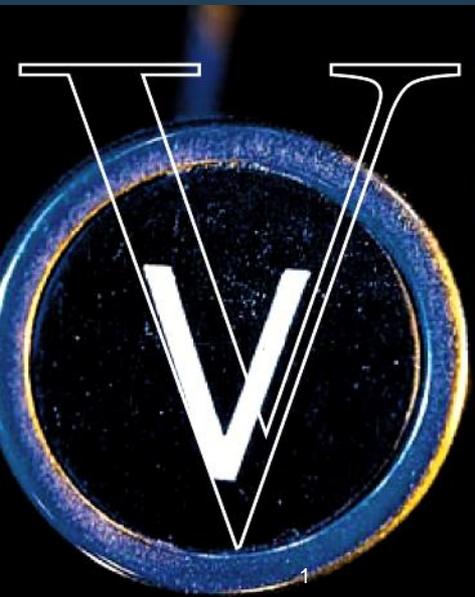
Jeffrey S. Tenenbaum, Esq., Venable LLP

Panelists:

William H. Devaney, Esq., Venable LLP

Joe Stephens, *The Washington Post*

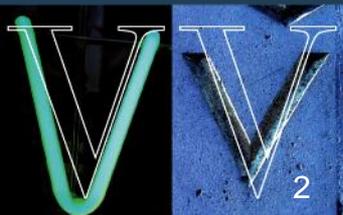
Nidhi Rao, CPA, CFE, CFF, CIA, BDO USA LLP



Upcoming Venable Nonprofit Legal Events

February 19, 2014 - [Implementing a Bring-Your-Own-Device Policy: What Your Nonprofit Needs to Know](#)

March 20, 2014 - The OMB Super Circular: What the New Rules Mean for Nonprofit Recipients of Federal Awards (details coming soon)



Agenda

- Recent Examples of Nonprofit Fraud and Embezzlement
- Why Does Employee Fraud Occur?
- Why Are Nonprofits Frequently the Victims of Fraud and Embezzlement?
- Effective Compliance Programs
- Controls Measures to Reduce the Risk of Fraud
- What to Do If an Issue Is Discovered?





Recent Examples of Nonprofit Fraud and Embezzlement

American Legacy Foundation

- In November 2013, Sen. Charles Grassley (R-Iowa), ranking member of the Senate Judiciary Committee, opened an investigation into the Washington, D.C.-based 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 *Post* report, the executive – who was in charge of both ordering computer equipment and checking it in as being received – 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 of the matter 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 *Post* reported that in 2011, the Vassar Brothers Medical Center in Poughkeepsie, New York reported a loss of \$8.6 million through the "theft" of certain medical devices.



Project Genesis, Inc.

- On October 12, 2013, the former CFO of Project Genesis, a Connecticut nonprofit organization that serves people with disabilities, was sentenced to 33 months' imprisonment after embezzling more than \$348,000 from the organization over a three-year period.
- The former CFO stole the organization's funds by keeping terminated employees on the payroll and then transferring their salaries to his personal bank account.



American Red Cross (NY Chapter)



**American
Red Cross**

- 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, Oklahoma, 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 for a total of more than \$1.35 million and embezzled more than \$200,000 from a thrift store operated by the nonprofit.



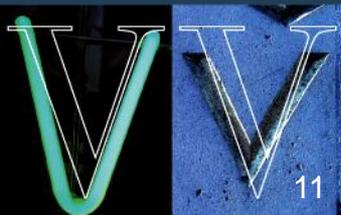
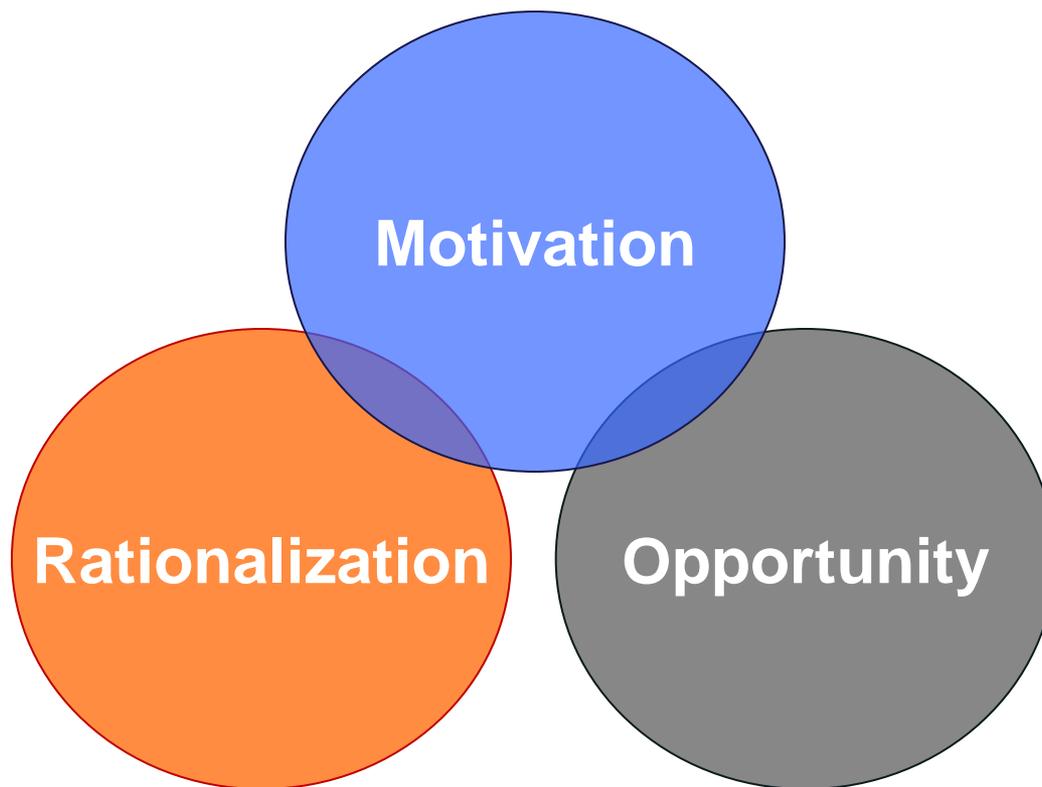
Global Fund to Fight AIDS, Tuberculosis and Malaria

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



Why Does Employee Fraud Occur?

Three Key Factors



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

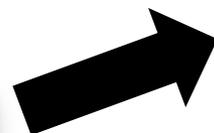
- The employee finds a way to rationalize the fraud.
- Such rationalizations can include perceived injustice in compensation as compared to their colleagues at for-profit enterprises, unhappiness over promotions, the idea that they are simply “borrowing” from the organization and fully intend to return 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 that allows him or her to believe the fraud can be committed and also successfully concealed.



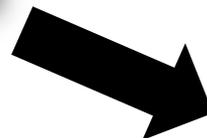
Why Are Nonprofits Frequently the Victims of Embezzlement?



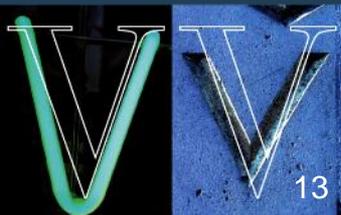
Management and board members are often more trusting



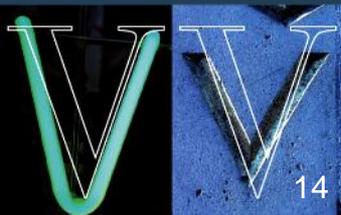
Less stringent financial controls for nonprofits



A belief that audits will catch any fraud



Set the Tone at the Top



Effective Compliance Programs

- The best way to prevent embezzlement and to protect an organization given the nature of respondeat superior liability is a comprehensive and vigorous compliance program that must be more than a “mere paper program.”
- Any effective compliance program will:
 - Be tailored to the specific organization, such that the controls mitigate the risks inherent in that organization’s business and address any applicable government regulations and industry standards.
 - 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.



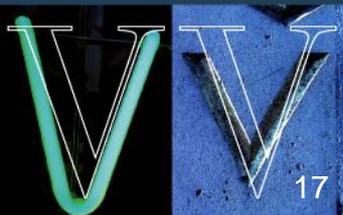
Effective Compliance Programs (cont'd.)

- Be owned by senior management. Management must be proactive. The Board must have ultimate oversight and control of the program.
- Provide for regular education and training for directors, management, employees, volunteers, and staff.
- Be regularly monitored and audited to ensure that it is working.
- Contain effective means to report violations and concerns, such as whistleblower hotlines or other anonymous reporting mechanisms.
- Provide for 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.
- Require that appropriate steps are taken if a crime occurs.
- Address any control weaknesses uncovered.



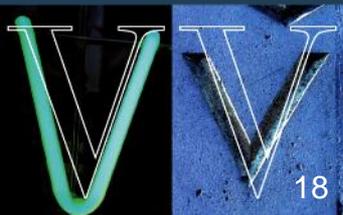
Role of the Board

- 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; and
 - 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 that degree of diligence, care, and skill which ordinary prudent people would exercise under similar circumstances.



Role of the Board (cont'd.)

- 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.





Control Measures to Reduce the Risk of Fraud

Fraud Risk Assessments

- 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 session 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.



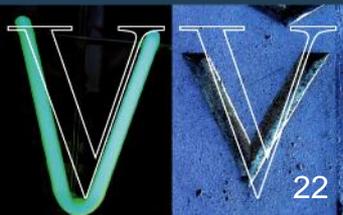
Segregation of Duties

- One individual should not be responsible for an entire financial transaction.
 - Record; Reconcile; Custody of Assets; Authorization
- Money Coming In: No one person should be responsible for receiving, depositing, recording, and reconciling the receipt of funds.
- Money Going Out: No one person should be responsible for authorizing payments, disbursing funds, and reconciling bank statements.
- Require employees who hold financial positions to take vacation.
- Utilize compensating controls if the organization does not have enough staff on hand to segregate these duties.
 - A board director or officer could receive and review the bank and credit card statements.



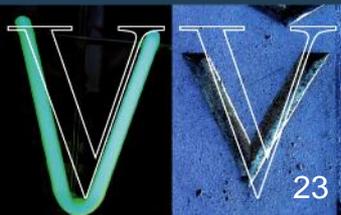
Double Signatures & Authorizations

- Multiple layers of approval will 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.
- With 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 request 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.

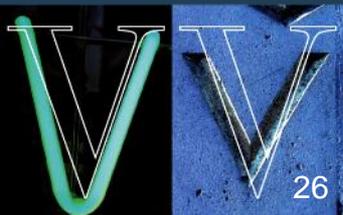
■ Fixed Asset Inventories

- 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.



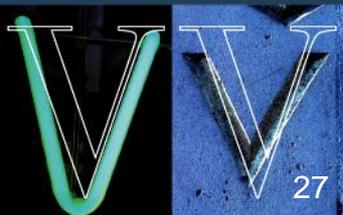
Automated Controls

- 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).
- Require physical access codes.
- Set system passwords.
- Use notification and alert services to alert the organization of possible debits to its accounts.
 - Positive pay exceptions notifications
 - Wire notifications (incoming/outgoing)
 - ACH Fraud Filter notifications
 - Balance threshold notifications



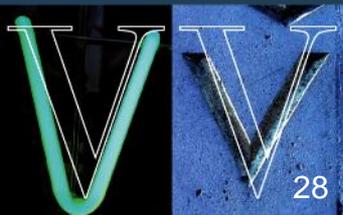
Conduct Background Checks

- Background checks on new employees and volunteers are important. Many organizations skip this basic step.
- The Association of Certified Fraud Examiners reports that 7 percent 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 a manner in which to contact a board member in the event 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.





What to Do If an Issue Is Discovered?

What to Do If an Issue Is Discovered?

- Selection of Investigative Team
- Evidence Preservation
- Evidence Gathering
- Background Checks in an Investigation
- Interviews
- Reporting
- Remediation



Selection of Investigative Team

When selecting the investigative team consider the:

- Investigative team's relationship with the suspect or the whistleblower (the investigator should never be the suspect's supervisor)
- Investigative team's position within the organization
- Role of the suspect's supervisor in the investigative team
- Need for engaging external counsel, forensic accountants, and other investigative consultants
- Attorney-client privilege



Evidence Preservation

- Preserve any potential evidence:
 - Pull back-up tapes
 - Preservation order
- Triage of potential evidence and target may include the following:
 - Placing the target on a leave of absence
 - Restricting his/her access to the organization's internal computer network and to its books and records
 - Organization should exercise caution and verify that these steps are taken in accordance with the company's policies and procedures/laws

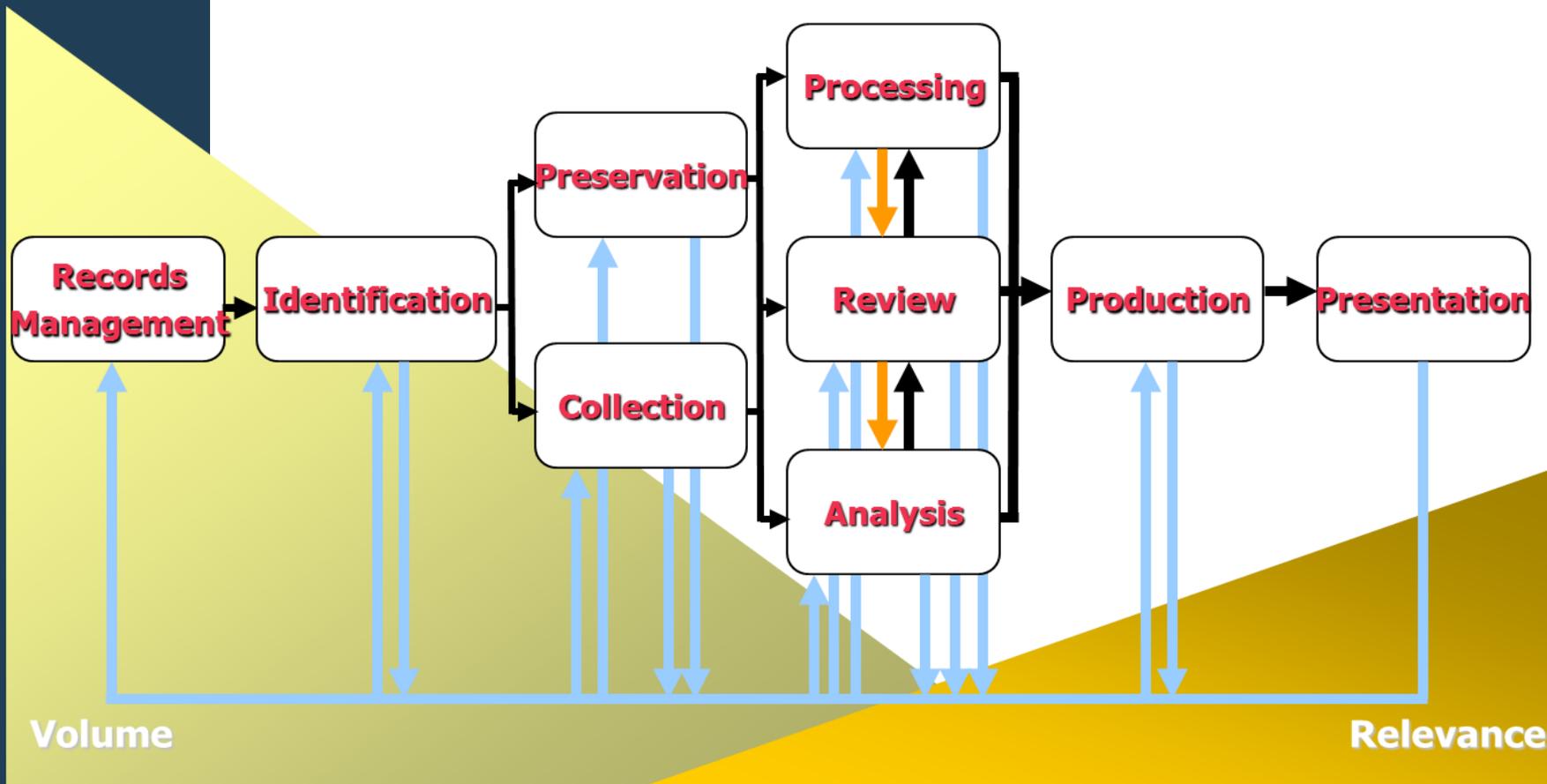


Evidence Gathering

- Document chain of custody of documents and materials
- Electronic Evidence
 - Electronic Discovery Lifecycle - EDRM
- Background Checks
- Interviews



Evidence Gathering



Source: Socha Consulting and Gelbmann & Associates.



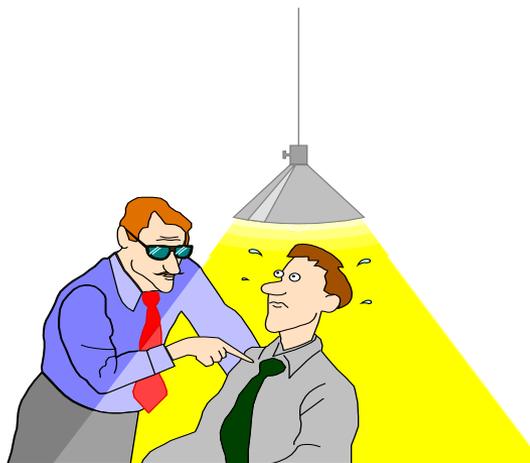
Background Check in an Investigation

- Conduct statewide criminal search as well as in the counties of residence/employment.
- Verify professional license and whether there has been any disciplinary history/sanctions by regulatory authorities.
- Conduct civil record, judgment, and lien searches in all jurisdictions linked to the subject.
- Use a combination of databases, plus free state record sites, as well as field investigators and sources.
- Don't limit a background check to an Internet search or to a compilation of raw data obtained from a search engine.
- Analyze the data in the context of the facts surrounding the fraud allegations being investigated.



Interviews

- Consider the timing of when the target is interviewed during the investigative process.
- Interviews are conducted by two investigators.
- Do not promise confidentiality “*Upjohn Warnings.*”
- Do not refuse to allow an employee to leave an interview.



Reporting

- Considerations can include the following:
 - Oral vs. Written/Privilege
 - Preparer
 - Distribution of the report
 - Facts, quantum, and circumstances
 - Should not contain recommendations for disciplinary actions or conclusions of guilt



Remediation

- Root cause analysis
- Remediation of internal controls
- Need for new policies and procedures
- Training
- Disciplinary action



Questions?

Jeffrey S. Tenenbaum, Esq.

jstenenbaum@Venable.com

t 202.344.8138

William H. Devaney, Esq.

whdevaney@Venable.com

t 410.244.7499

Joe Stephens

Joe.Stephens@washpost.com

t 202.334.6723

Nidhi Rao, CPA, CFE, CFF, CIA

NRao@bdo.com

t 301.634.4966

To view Venable's index of articles, presentations, recordings and upcoming seminars on nonprofit legal topics, see www.Venable.com/nonprofits/publications, www.Venable.com/nonprofits/recordings, www.Venable.com/nonprofits/events.

