The Insider Threat
2013 Nonprofit Accounting & Auditing Update

By

Andrew Laflin, CPA
CliftonLarsonAllen LLP

Patrick Laflin
Federal Bureau of Investigation

CliftonLarsonAllen

cliftonlarsonallen.com

Occupational Fraud

Presentation Focus: **Occupational Fraud**

Definition: The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

Occupational Fraud is far and away the largest source of fraud loss

Source – 2012 Report to the Nation on Occupational Fraud and Abuse

Objectives

At the end of this session, you will be able to:

- Understand the latest fraud risks affecting nonprofit entities
- Be aware of the impact fraud has on your organization
- Identify methods that will help mitigate your fraud risks
- Gain a deeper understanding of the risks and consequences of insider theft of sensitive information

How 'big' is Fraud? Typical organization loses 5% of revenues per year due to fraud. Translates to estimated $3.5 Trillion Worldwide*

** Source – 2012 Report to the Nation on Occupational Fraud and Abuse*

Reference Materials

- To research your organization's likely risks given industry and size look to **The 2012 ACFE Report to the Nation**
  - Best source to research organizational exposure by industry and firm size; 2012 version available online free at **http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf**

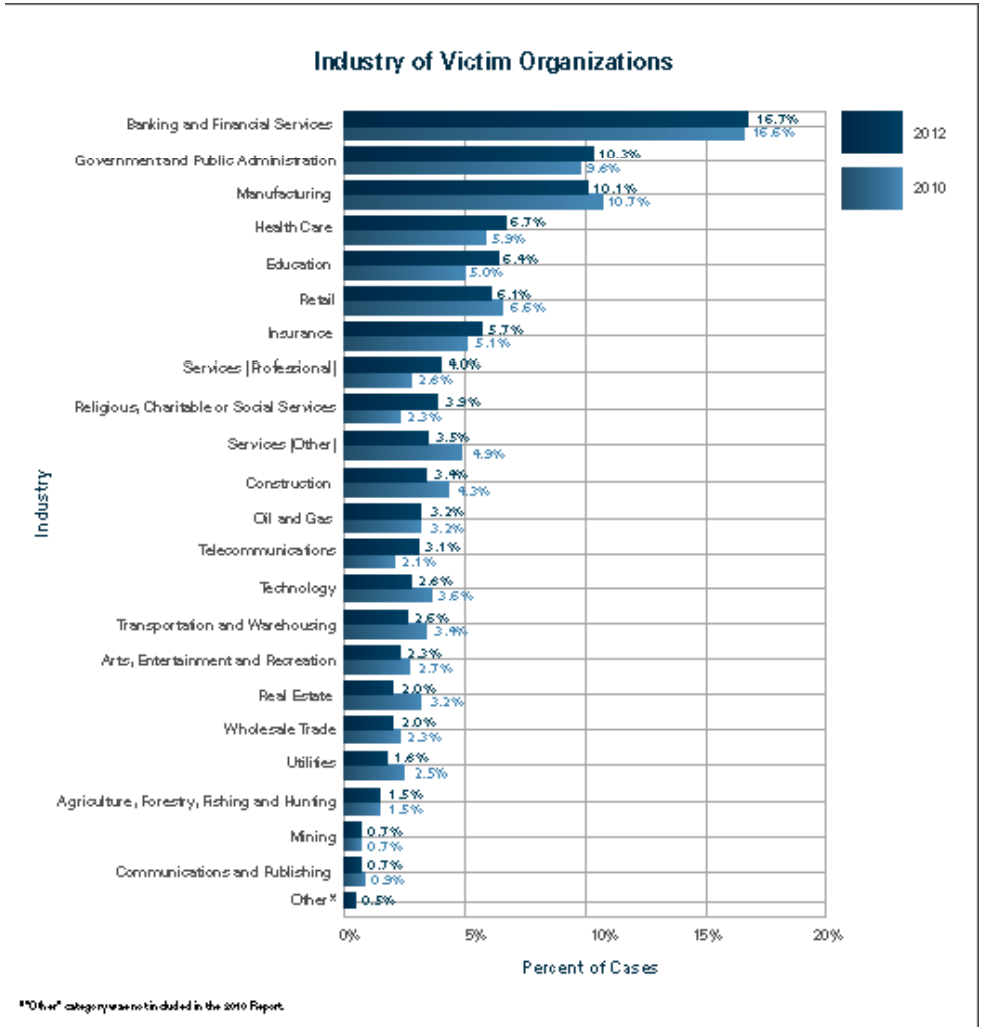
Types of Occupational Fraud - Definitions

- Occupational Fraud can be broken down into three main categories:
  - *Corruption* schemes, in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit (e.g., schemes involving bribery or conflicts of interest)
  - *Financial statement fraud* schemes, in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports (e.g., recording fictitious revenues, understating reported expenses or artificially inflating reported assets)
  - *Asset misappropriation* schemes, in which an employee steals or misuses the organization's resources (e.g., theft of company cash, false billing schemes or inflated expense reports)

Who Commits Fraud (All Industries)?

- Male or female?
- Over 40 or under 40?
- Employees, managers, or executives?
- What was the most common position held by the fraudster?
- High school graduate and some college, bachelor's degree, or post-graduate degree?

Types of Frauds and Frequency by Industry



Source – 2012 Report to the Nation on Occupational Fraud and Abuse

Fraud Schemes – Education

Education 88 Cases		
Scheme	Number of Cases	Percent of Cases
Billing	28	31.8%
Expense Reimbursements	23	26.1%
Corruption	21	23.9%
Skimming	19	21.6%
Payroll	13	14.8%
Check Tampering	11	12.5%
Cash on Hand	11	12.5%
Cash Larceny	8	9.1%
Non-Cash	7	8.0%
Register Disbursements	5	5.7%
Financial Statement Fraud	4	4.5%

Source – 2012 Report to the Nation on Occupational Fraud and Abuse

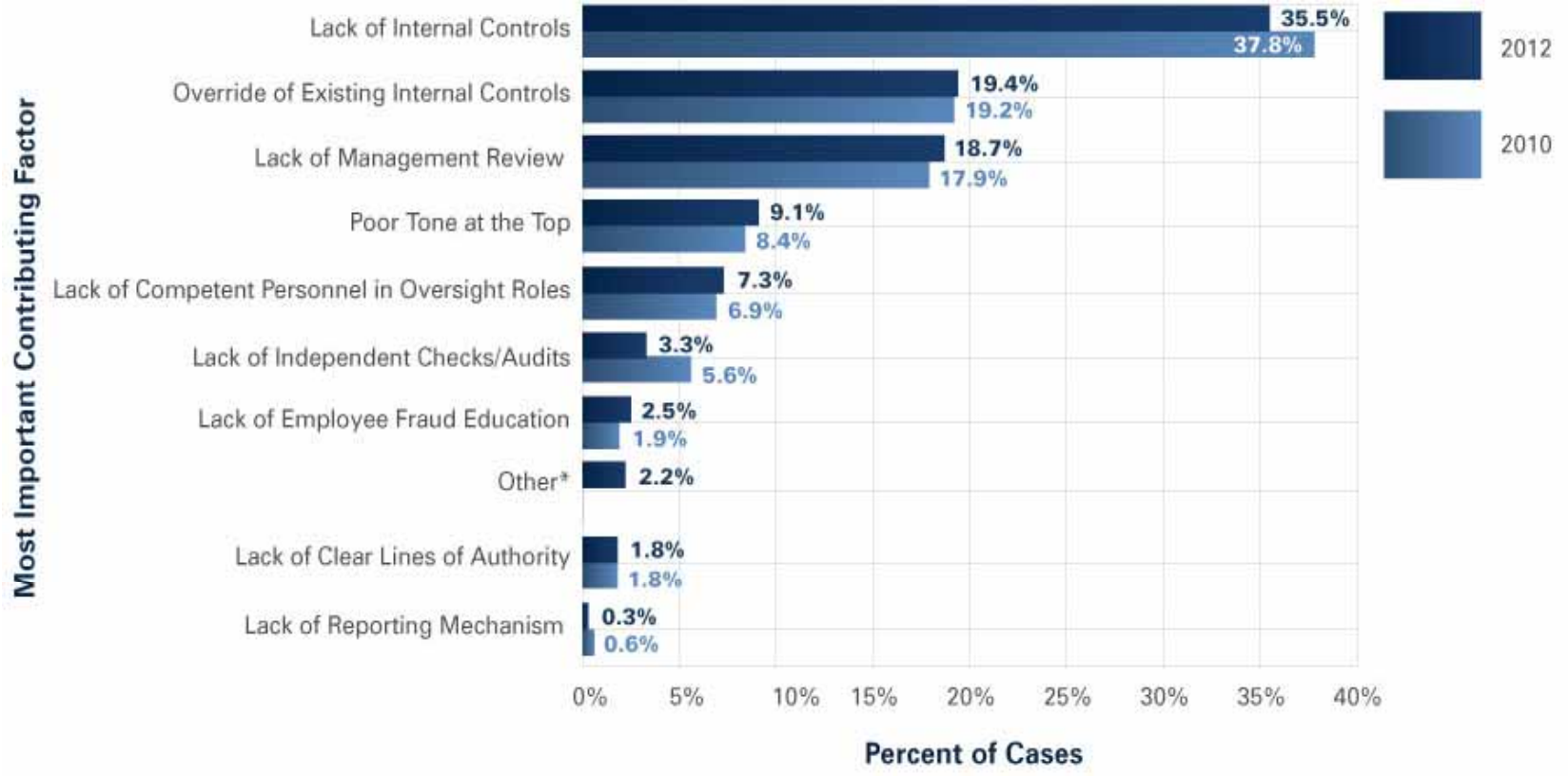
Fraud Schemes – Religious, Charitable & Social Services

Religious, Charitable or Social Services 54 Cases		
Scheme	Number of Cases	Percent of Cases
Billing	28	51.9%
Check Tampering	18	33.3%
Expense Reimbursements	17	31.5%
Skimming	12	22.2%
Corruption	12	22.2%
Cash Larceny	11	20.4%
Payroll	8	14.8%
Cash on Hand	7	13.0%
Non-Cash	6	11.1%
Register Disbursements	3	5.6%
Financial Statement Fraud	3	5.6%

Source – 2012 Report to the Nation on Occupational Fraud and Abuse

Factors that Contribute to/Allow Fraud

- Primarily internal control weaknesses:



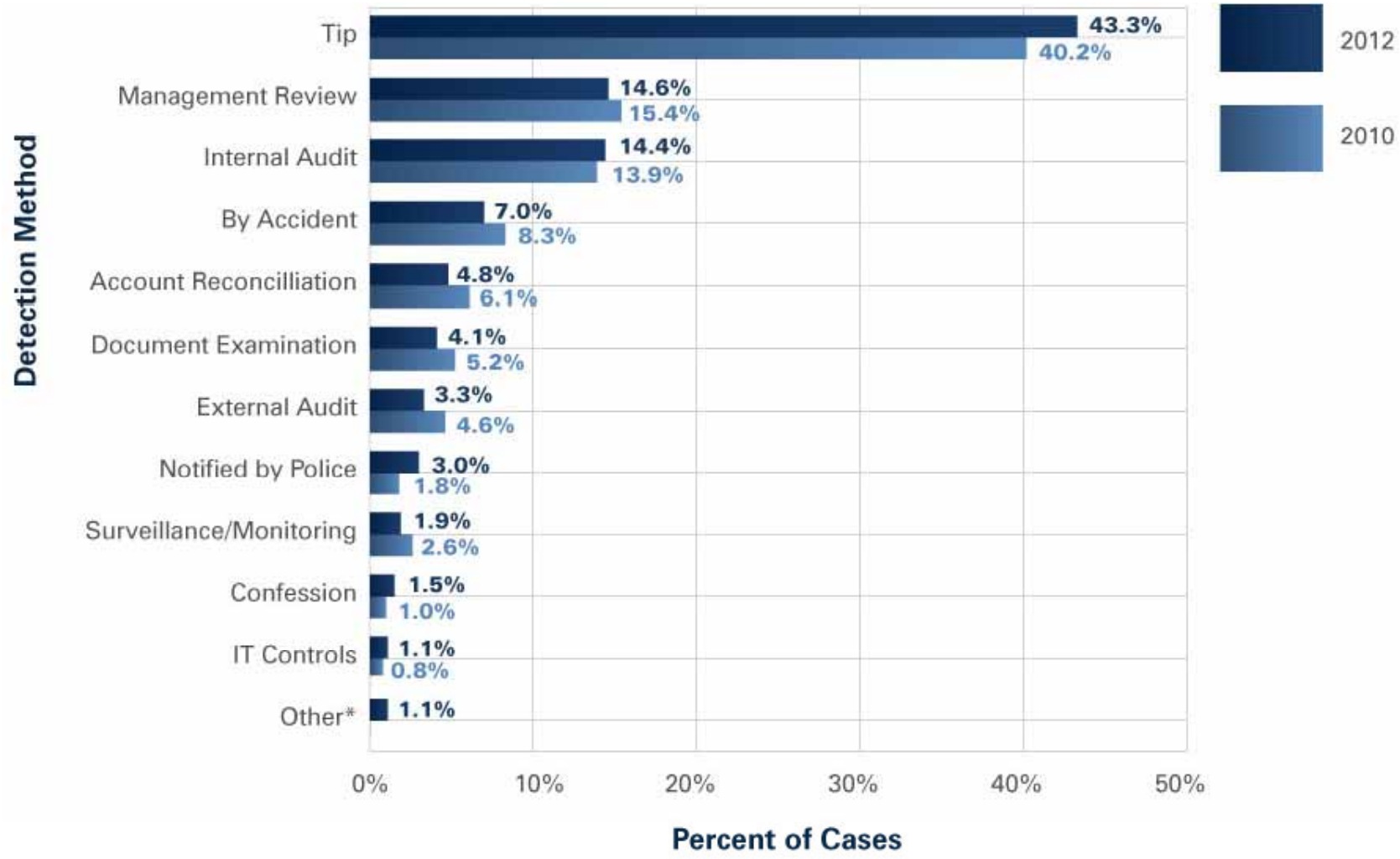
Source – 2012 Report to the Nation on Occupational Fraud and Abuse

Red Flags – Behaviors to Watch For

Source – 2012 Report to the Nation on Occupational Fraud and Abuse

CliftonLarsonAllen

Anti-Fraud Measures



Source – 2012 Report to the Nation on Occupational Fraud and Abuse

Anti-Fraud Measures (Used vs. Used Successfully)

- Across all organizations, **Occupational Frauds are more likely to be detected by a tip** than by other means such as internal audits, external audits or internal controls

- Make detection easier – have an anonymous tip line

Scenario #1 – The "ArtsTheft"

- Founded in 1984, ArtsQuest is a Bethlehem, PA-based nonprofit organization dedicated to providing access to exceptional artistic, cultural and educational experiences for residents of the Lehigh Valley region of Pennsylvania and beyond. The 501 (c)(3) supports this mission via the presentation of performing and visual arts, farmers' markets and healthy living initiatives, youth and community programming, and a variety of cultural events

Scenario #1 – The "ArtsTheft"

- For nearly three decades, ArtsQuest has presented festivals, cultural experiences and educational and outreach programs that aid in economic development, urban revitalization and community enrichment. Through festivals such as its flagship event, Musikfest; the Banana Factory community arts and education center; and the new ArtsQuest Center and SteelStacks arts and cultural campus, the nonprofit's programming reaches more than 1.3 million people annually, with more than 80 percent of this programming offered to the community free of charge.

Scenario #1 – The "ArtsTheft"

- Gift shop employee Tynesha Gilmore entered fake product returns and pocketed the cash from those fake returns
- Over an eight-month period, authorities say, Gilmore stole more than $3,000 from ArtsQuest. Scott Hough, director of event services for the nonprofit, went to police after management discovered the thefts, court papers say

Scenario #1 – What Have We Learned

- Require periodic inventories
- Review and reconciliation of product returns

Scenario #2 – the House of *Dis*Grace

- the House of Grace of the Adirondacks, a Glens Falls, N.Y. non-profit provides in-home hospice care to patients battling terminal illness

- From its website: “House of Grace receives no funding. As a nonprofit organization, we are totally dependent on the generosity of our community for support. We do request a room donation. With that support House of Grace will continue its much needed mission”

Scenario #2 – the House of *Dis*Grace

- Robert Spratt's job was supposed to be to raise money and awareness for the House of Grace

- According to Glens Falls Police, Pratt stole more than $26,000 between October 2011 and June of this year. He reportedly falsified checks written to himself, claiming to have paid for a range of services and then sought to be reimbursed

Scenario #2 – What Did We Learn

- Evaluate expense reimbursement policy
- Ensure all checks written for payment are supported by adequate documentation
- Ensure proper approval on all check disbursements
- Financial analytical review analysis (periodic budget to actual and prior period to current period comparisons)

Scenario #3 – The Bellringer

- Monroe, LA police arrested a 32-year-old woman after she allegedly misused credit cards issued to the local Salvation Army to accumulate more than $30,000 in charges

- Routine accounting procedures noted a spike in the monthly credit card bills and initiated a fraud audit

Scenario #3 – The Bellringer

- A former food services director of the Salvation Army in Joplin, MO pleaded guilty Monday to fraudulent use of credit cards belonging to the charity organization
- Stephen D. Lewallen, 35, was charged in December 2011 after its was discovered that the limit had been exceeded on one of the organization's charge cards with Wal-Mart
- Charges on a statement with an end date of Nov. 29, 2011, totaled $2,656.15. But the business manager told police at the time that for the card to be over its limit, about $18,000 in fraudulent charges would have had to have been made, according to the affidavit

Scenario #3 – What We Learned

- Reduce or eliminate high-level individuals with credit cards
- Strengthen oversight and review of credit cards
- Evaluate whether controls can be circumvented around credit cards
- How many card holders are there at your organization?

Scenario #4 – The HR Nightmare

- The Arc Mercer's human resources director has been arrested and charged with stealing more than $100,000 from the nonprofit organization over three months
- Christopher English, 32, of Delran continued to generate paychecks for employees who had resigned or were terminated and deposited the checks into a bank account, the prosecutor's office said

Scenario #4 – The HR Nightmare

- Arc Mercer officials said they were transitioning to a new payroll vendor in January when management uncovered some irregularities
- In recent weeks they identified several payments to employees who should not have been on the payroll, being sent via direct deposit to a single account, the statement said

Scenario #4 – What We Learned

- Prompt removal of terminated employees from the payroll system
- Remove administrative access rights to those in a supervisory capacity (Payroll Manager, HR Director, etc.)
- Review of pay register each pay period by someone other than preparer

Scenario #5 – Don't Click That Link!!

- MECA Mission: Relieve the burdens of government through management and operation of government owned convention, sports and entertainment facilities located in Omaha, Nebraska

Scenario #5 – Don’t Click That Link!!

- Cyberthieves reportedly funneled $217,000 from MECA
- An employee at MECA fell for a phishy e-mail that unleashed a malware attack that subsequently provided hackers with access to the organization’s payroll system
- From there, cyberthieves hijacked the system's login and password credentials, allowing them to add their own hires to the payroll. Those hired individuals or money mules, once on the payroll, received payment transfers from MECA’s bank account

Scenario #5 – Don’t Click That Link!!

- Before the attack, MECA allegedly passed on security options offered by First National Bank of Omaha, including one option that required two employees to sign off on every funds transfer
- "We had declined some of the security measures offered to us," Lea French, MECA's chief financial officer, reportedly told Krebs. "We thought that would be administratively burdensome, and I was more worried about internal stuff, not somebody hacking into our systems."

Scenario #5 – What We Learned

- Implement security features offered by your bank, even if construed as administratively burdensome
- Use positive pay lists for both payroll and non-payroll disbursements, if possible
- Implement an incident response plan
- Educate employees about taking proper information security measures
- Periodically perform vulnerability assessments

Questions and Comments

Andrew Laflin, CPA
Manager
CliftonLarsonAllen LLP
(813) 384-2711 (office)
(813) 784-3140 (cell)
andrew.laflin@cliftonlarsonallen.com

CliftonLarsonAllen