

FRAUD RISKS IN GOVERNMENTS

Presented by:

Michael Michelsen, CPA



Specialization

What is Forensics?



What is Forensic Accounting?

“CSI” Television Show



What does it look like?



What will you do?



When this happens...*ON YOUR WATCH?*

EFFECTS OF FRAUD

Impact of Fraudulent Activity



Fraud Survey

What is your “acceptable” fraud loss?



Medicaid Program \$1.4 Billion

What is your “acceptable” fraud loss?

10%

\$140,000,000

Source: Idaho Attorney General 2013
U.S. Department of Health and Human Services 2013

Fraud Survey – Government

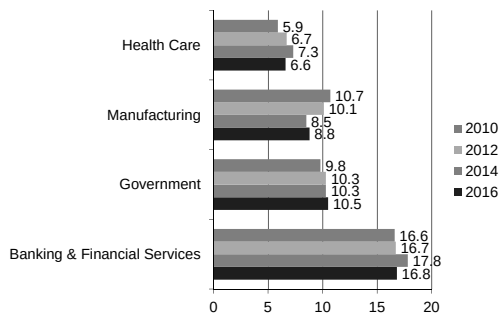
- Estimated 3/4 of organizations fall victims of fraud
- Government rates #2 on industry list
- 18-24 months before detection
- 5% of total revenue
- Median loss \$150,000



\$3.7 trillion annual fraud loss globally

Source: ACFE 2016 Report to the Nations

Victim Organizations – by Industry



Source: ACFE 2010-2016 Report to the Nations

RAISING SUSPICIONS

Recognizing the Signs of Fraud



Foundations for Internal Fraud

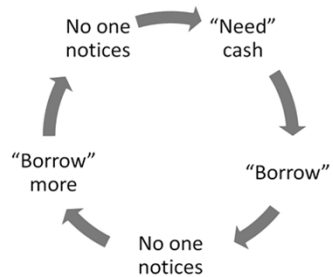
•Employee Traits

- Financial pressure
- Exploitable opportunity
- Rationalization available

•Most Common Perpetrator Traits

- Most “trusted” employee
- Star performer
- Long term employee

How People “Cross the Line”



Red Flags – Financial

- Cash flow problems
- Records not produced upon demand
- Source documents lost
- Problems with financial statements
- Unexplained lack of profit



Red Flags - Employee

- Employee does NOT miss work
- Family Issues
- Drugs/Alcohol/Gambling
- Living Beyond Means



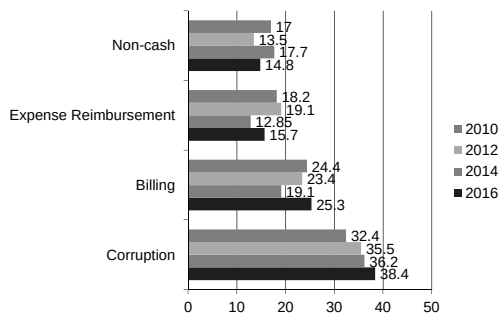
TYPICAL FRAUDS

Top Fraud Schemes

Is it just the money?

Do you need to be concerned?

Government Fraud Trends



Source: ACFE 2010-2016 Report to the Nations

Government Fraud Trends

- **Corruption Schemes**
 - Use of influence for personal benefit
- **Billing Schemes**
 - Payments of inflated or fictitious invoices
- **Expense Reimbursements**
 - Reimbursement for inflated/fictitious expenses

Expense Report – Busted!



What will you do?

Fraud Detection:

Learn how fraudsters conceal their schemes
Focus on known methods first



Internal Control Weaknesses

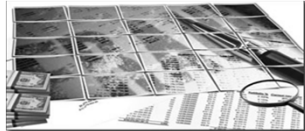
Accounts Receivable - Example:

- Key supervisor makes daily bank deposit
- Most likely to succeed in fraud



Major Internal Control Weaknesses

- **Key employees do too much**
Access to and control all revenue
- **Managers do not monitor their work**
Employees operate in secret while in plain sight of everyone
- Why?.....



Trust but Verify Concept

Managers use “blind trust”

- Tell employees what to do
- Expect them to do it
- Never monitor actions to see if expectations are met

Managers should use “trust but verify”

- Monitor employee actions
- Chinese saying: “It’s OK to trust employees, just always keep one eye open!”

Employee Types

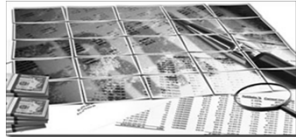
- Two types of employees:
 - **Doers** - most internal controls exist here
 - **Reviewers** - few or no controls
 - Managers monitor supervisors differently
 - Not reviewed like subordinates
- Fraudsters ignore/compromise internal controls
- Fraudsters do not play by the rules

Crossing the Line – Honest to Dishonest

- What happens when – manager does not monitor supervisor, and the supervisor makes the daily bank deposit?

Key employee often crosses line to become dishonest
Key employee manipulates deposit detail
Key employee defrauds employer by misappropriating

- **Result is fraud!**

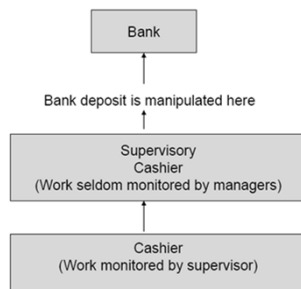


Internal Control Risks

- Expect doers to follow rules
- Expect supervisors to monitor work of doers
- Supervisor makes bank deposit
- We think we are done.....wrong assumption!



Bank Deposit Process



A/R Revenue Fraud #1 Cause

Internal control failure found in **every** revenue fraud:

Key employee who makes daily bank deposit is not monitored



“At Risk” Employees

- Work Habits of “At-Risk” Employees - who do you know?

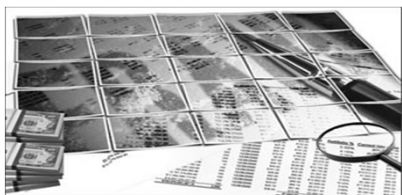
Arrives early to work and leaves late
Works nights & weekends
Does not take vacations or sick leave
Reports to office during brief absences
Asks others to “hold work” while away from office



Identifying “At Risk” Employees

Work Habits of “At-Risk” Employees – conclusion:

Key Issue - **control of work environment**



“At Risk” Use of PC’s

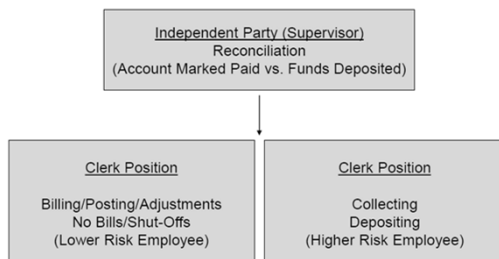
- Personal computers used for accounting purposes
 - Small organizations use PC’s
 - No internal controls – no audit trail
- Resulting fraud – missing or destroyed documents



“Off-Book” Accounts Receivables

- A/R collection of funds from current account balances
 - Delinquent A/R sent to collection agency – limited staff
 - Delinquent A/R not recorded in accounting system
 - Delinquent A/R not reported on financial statements
- Resulting fraud – revenue from delinquent A/R is prime target
 - Lack of monitoring by managers

A/R Duties & Responsibilities



Segregation of Employee Duties

- Three person operation – **ideal controls**
 - Billing & posting
 - Collecting & depositing
 - Independent supervisor reconciles accounting information
- Independent Reconciliations
 - Paid accounts marked "paid" – amount of bank deposit
 - Payment reconciliation of records vs. money
- Fraud quickly detected – unless review is performed out of sequence

Segregation of Employee Duties

- Two person operation – **some controls**
 - Billing & posting
 - Collecting & depositing
- Independent reconciliations – who should reconcile and why?
 - Billing & posting
 - Generally no access to money
 - Lower risk** - will generally report differences
 - Collecting & depositing
 - Higher risk** - will not self-report differences

Segregation of Employee Duties

- One person operation – **no controls**
- One person does everything
- Independent monitoring is required
 - Manager
 - Board member or governing body
 - Outside volunteer

Segregation of Employee Duties

- **Danger** of employee duties:
- **Internal controls “self-destruct” at lunch & breaks –**
Record keepers become relief cashiers



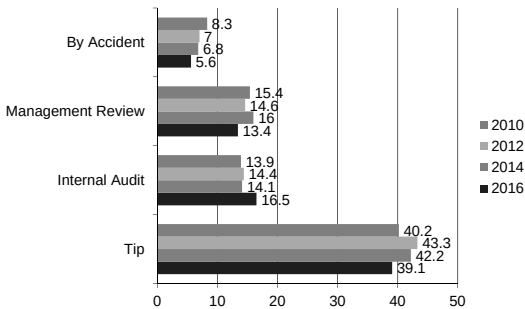
Secrets of Detection

- Study internal controls system -
Focus on employees who perform too many tasks
Determine if managers monitor their work
- If PC'S are used for accounting -
Compare manual & computer accounting records for agreement
Confirm transactions with customers
Obtain copies of checks & review endorsements
Subpoena employee's personal bank records

Secrets of Detection

- Additional review steps include -
Observe employee changes in behavior/attitude
Observe employees with access/control & make deposits
Observe & listen others to identify “at risk” employees
Inquire about who performs relief cashier duties
Determine if employees are required to take vacations &
cross-train employees by switching duties
Verify if there is a “last look” policy to analyze daily
bank deposit contents after being prepared/before actual deposit
Search for “off-book” accounts receivables

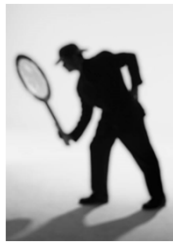
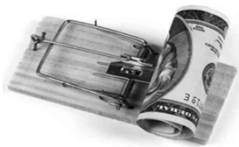
Detection of Fraud Schemes



Source: ACFE 2014 & 2016 Report to the Nations

Fraud Prevention

Prevention
is easier than
Detection



Fraud Prevention

- *Basic principle:*
 - People rarely commit fraud if they think they will be caught
- *Perception of detection:*
 - Most effective deterrent to fraud



Increase Perception of Detection

- ***“Tone at the Top”***

- Managers need to communicate the idea that they are serious about their fraud detection and prevention efforts

- ***Employee Education***

- Internal controls for monitoring employees
- Company fraud (ethics) policy



Effective System of Internal Control

Segregation of duties:

- Authorization
- Record keeping
- Custody of assets



Physical control over assets and records

- Secured check stocks
- Controlled access to inventory

The Do's of Internal Controls

- Top level Reviews of Actual Performance
- Reviews by Management at the Functional or Activity Level
- **Management of Human Capital**
- Controls Over Information Processing
- **Physical Control over Vulnerable Assets**
- **Establishment and review of Performance Measures and Indicators**

The Do's of Internal Controls

- Segregation of Duties
- Proper Execution of Transactions and Events
- **Accurate and Timely Recording of Transactions and Events**
- Access Restrictions to and Accountability for Resources and Records
- Appropriate Documentation of Transactions and Internal Control

The Do's of Internal Controls

- Change computer passwords
- Periodic analysis
- Require vacations
- Cross train employees
- Budget vs. actual review

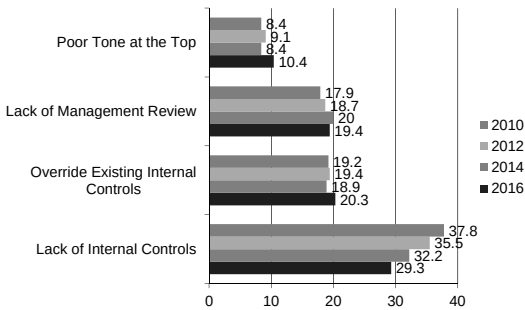


The Don'ts of Internal Control

- Subordinates approve boss' travel or expense reimbursements
- Too many controls
- Inversely – not enough controls
- No reconciliations
- Too much trust in one person



Primary Internal Control Weaknesses



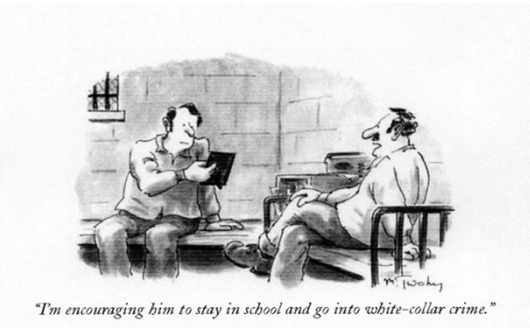
Source - 2012 ACFE Report to the Nations

Effective System of Internal Control

- **Independent checks** on performance
 - Review & follow-up of financial performance indicators
 - Documentation of follow-up and resolution of issues
- **Reporting program** (hotline, open-door policy)
 - How is program communicated to staff?
- **Vigorously pursue** dishonest acts



The Future of Fraud





What will you do?



When this happens...*ON YOUR WATCH?*



You can make a difference

Choose to do right
Do your best
“Platinum” rule





Questions & Comments?

Michael Michelsen

801.456.5457

mmichelsen@eidebailly.com
