Identifying Occupational Fraud Risks and Fraud Prevention Control

Chamber of Commerce

26 May 2016
Occupational Fraud Risks and Fraud Prevention Controls

Goals for today:

• An introduction to understanding motivations and techniques used to commit business fraud, and how best to prevent and detect fraud

Translates into

➢ Identifying occupational fraud risks
➢ Identifying fraud prevention controls
➢ Tips for business owners on how to identify the red flags of fraud, and introduce the controls to best prevent and detect fraud
Occupational Fraud Risks and Fraud Prevention Controls

Presentation objectives:

• To understand how and why occupational business place fraud occurs.

• Techniques and procedures used to prevent fraud.

• Examples of red flags used to detect fraud.

• How to establish a culture of fraud awareness, prevention, and detection.

• What to do when your business is the victim of fraud

“At any given moment, there is a certain percentage of the population that’s up to no good.”
J. Edgar Hoover
Fraud: definition
Multiple definitions

• Definition A: Any deliberate act designed to result in unauthorized gain for an individual or an organization

• Definition B: Intentional act by one or more individuals, involving the use of deception to obtain an unjust or illegal advantage

• Definition C: 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)

  ➢ Fraud in this sense is broader than in the legal sense
  ➢ Fraud is not just about misappropriation of assets but can equally be about deliberate misstatement
  ➢ It might be, but doesn’t have to be a criminal offense (e.g. financial misrepresentation)
  ➢ Impact of business fraud within SMEs has much wider ethical implications
Significant Occupational Fraud Risk Factors

- Lack of detailed formal written policies and procedures
- Lack of segregation of duties
- Lack of control over transaction cycles
- Unreconciled accounts, lack of review of reconcilements
- Incorrect, incomplete, erroneous financial reporting; missing financial records
- Untimely preparation of financial records
- Lack of employee vacations
- Lack of management oversight
- Bonus or incentive plans
- Employee addictions
- Tone at the top

- Lack of internal control reports from data processing systems
- Complex transactions
- Rapid growth
- Corporate credit cards
- Employee financial problems
- Inactive supervision
- Lack of audit/verification
- Lack of employee training
- High employee turnover
- Unlocked cash drawers!
Impact of occupational fraud on business victims

Damage to victims goes beyond the simple dollars stolen/diverted. Consider the ‘real’ full costs ...

• Investigation costs
• Diverted management time, distraction to the business
• Disciplinary process costs
• Regulatory penalties
• Recruitment of replacement staff
• Reputational damage, loss of public confidence
• Effect on attracting new customers, employees, suppliers, etc
• Damage to relationships
• Sagging staff morale
What do you think the profile of a fraudster is?
The typical fraudster?

The myth

- Never takes holiday
- Always broke
- Male
- Unpopular, boring
- Someone whom you always had your doubts about
- Steals from petty cash
- ‘John’ in Accounts
The typical fraudster?

The reality

- Your ‘mate’/golf partner
- Well-liked
- Takes nice holidays
- Intelligent
- No obvious reason to commit fraud

Four-fifths of executives admit to cheating on the golf course!!
### Department / Position in organization

<table>
<thead>
<tr>
<th>Principle departments</th>
<th>Common characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>Trusted employee / manager</td>
</tr>
<tr>
<td>Sales</td>
<td>Male 67% Female 33%</td>
</tr>
<tr>
<td>Operations</td>
<td>31-45 years old</td>
</tr>
<tr>
<td>Executive / Upper Management</td>
<td>With organization &gt; 1 years</td>
</tr>
<tr>
<td>Customer Service</td>
<td>No previous history of fraud</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Educated</td>
</tr>
<tr>
<td>Other (&gt;25%)</td>
<td>Collusion with outside parties</td>
</tr>
</tbody>
</table>

*Largest and longest frauds commonly committed by management*
### Characteristics of the White Collar Criminal

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Older (30 + years)</td>
</tr>
<tr>
<td>Family</td>
<td>An appearance of a stable family situation</td>
</tr>
<tr>
<td>Education</td>
<td>Above-average (post-graduate) education</td>
</tr>
<tr>
<td>Criminal record</td>
<td>Less likely to have criminal record</td>
</tr>
<tr>
<td>Managerial</td>
<td>Position of trust</td>
</tr>
<tr>
<td>Psycho</td>
<td>Good psychological health</td>
</tr>
<tr>
<td>Accounting</td>
<td>Detailed knowledge of accounting systems and weaknesses</td>
</tr>
<tr>
<td></td>
<td>Prior Accounting experience</td>
</tr>
</tbody>
</table>
Behavourial red flags – occupational fraud

Individuals

Typical fraudster behavioural red flags (with the benefit of hindsight!)

• Living beyond means / exorbitant lifestyle
• Financial difficulties (excessive debt)
• Unusually close associations with vendor/customer
• Control issues, unwillingness to share, excessive overtime
• Wheeler-dealer attitude, unethical corner-cutting
• Divorce/family problems, emotional trauma, etc
• Addiction problems, excessive drinking/betting, etc
• Permanently stressed out, irritable
• Vocal complaints about inadequate pay, low morale, oppression in the workplace ...
Behavourial red flags
Companies (management)

Fraud symptoms relating to an entity

• Unquestioning obedience of employees – ‘yes’ culture
• Organisation always in ‘crisis mode’
• Auditors (external/internal) ignored
• Poor corporate governance
• Complex structures and reporting lines
• Remote locations poorly supervised
• Poor commitment to ethics and internal control
• Limited or no rotation/segregation of duties
• Incentive schemes too closely linked to profit

... more relevant to larger businesses ...
Other warning signs
Non-exhaustive list ....

Other potential warning signs:

• Use of ‘non-obvious’ third parties
• Oral side agreements contradicting written documents
• Whistleblowers – internal/external
• Minority shareholder complaints
• Marketplace rumours, press comment
• Sudden changes in oversight teams
• Outsourcing of the accounting function
• ‘Too good to be true’ transactions
• Dominant CEO, weak CFO
• Poor, non-integrated systems

... more relevant to larger businesses ...
Types of business fraud?
Types of business fraud

Perpetrator

Individual

Company

Main types

Misappropriation of assets (embezzlement, theft)

Bribery, corruption

Fraudulent financial reporting
Fraud Tree (ACFE)
Explaining different terms

- **Corruption**: abuse of entrusted power for private gain
- **Bribery**: giving or offering of a bribe in the form of money or favor given or promised in order to influence the judgment or conduct of a person
- **Extortion**: practice of obtaining something, especially money, through force or threats
- **Embezzlement**: appropriation for one's own use of money or property entrusted to one's care
- **Theft (larceny)**: where property belonging to another is taken without that person's consent

... difference between embezzlement and theft:

- Fraudsters attempt to conceal embezzlement (false accounting entries, false records)
- Companies prime focus often on theft (physical security)

... meaning embezzlement is more dangerous
Why fraud?
Fraud Risk Triangle
What makes people commit fraud?

Pressure = Stimulus
Rationalize = Reasoning / Attitude
Opportunity = Opportunity
The Typical Workforce
Reality and myth

The myth
The reality

Honest
It all depends
Fraudulent
How honest are you?

- Insurance overstatement
- Tax manipulation
- Reward scheme manipulation
- Expense overstatement
- Large gifts
- Conflicts of interest
- Pilferage
- Fraud

Angel... Fallen...
Stimulus / pressure

Employee fraud

Employees / management against company

- Bonuses based on financial performance
- High financial debts and unusual financial situations
  - Gambling, Substance abuse (drugs, alcohol etc.)
  - Living beyond one’s means
  - Extensive investment speculations
  - High pressure and focus of management on financial result
  - Family pressures
- Job frustration; resentment against superiors
- Operating out of depth

KRyS-Global.com

23
Stimulus / pressure

Company fraud

Management on behalf of company

• Unfavourable economic conditions in the industry
• Reputational pressures - lay-offs, bad morale
• Heavy losses / investments that didn’t pay off
• Insufficient working capital / high debts
• Need to survive through a bad situation
• Share price falls
Rationalization

Reasoning, movements in attitude

• There is a belief that others are paying bribes to win contracts
• My targets are more difficult to achieve / unachievable
• Previous allegations of fraud within the organization were not properly investigated
• I need to make the numbers in order earn performance bonuses
• I need to maintain the impression I can afford a certain standard of living
• People afraid they might lose their jobs
• Bonuses not paid this year, but I’ve already spent the money
• Others are doing it, so it’s okay
• Autocratic management, resentment towards superiors
• Etc, etc, etc ....
Attitude / Reasoning

Justification for committing fraud

“My employer didn’t compensate me well enough, so I took what rightfully was due to me”

“I felt cheated and wanted revenge”

“I’m not hurting anybody”

“It was just a loan, I intended to pay it back”

“I needed the money”

“Everyone else was doing it”

“The company is rich enough and will not miss that small amount”

“The company owes it to me”

“The bribe was too tempting”

“I will stop as soon as I am out of these financial difficulties”
Opportunity

Opportunity, opportunity, ...

• Ineffective or no internal controls (lack of segregation of duties)
• Ineffective internal audit staff / compliance / risk management oversight
• Weak / decentralised management
• Frequent management changes
• Close associations with suppliers or competitors
• Firm always in ‘crisis mode’ – management by crisis
• Lack of accountability
• Related party transactions
• High staff turnover
Principle areas of business fraud?
Four main types of fraud

- Asset Misappropriation: Theft
- Asset Misappropriation: Embezzlement
- Bribery / Corruption
- Financial Statement Misstatement
Asset misappropriation
Theft

Examples:

• Stealing inventory
• Stealing other physical assets
• Stealing intellectual property
• Causing an entity to pay for goods not received e.g. including false expense claims
• Causing an entity to pay for services not received e.g. including false time entries
• Using an entity’s assets for personal purposes
• Purchasing items for personal use or resale
E.g. Purchases for personal use or resale

Description

- Items purchased by employee through his/her agency or company
- Intended for his/her personal use or for resale
- E.g. stationery, computers, computer parts, automobile parts, inventory

Red Flags

- High volume or unusual purchases of ‘consumer items’ or items suitable for personal use or resale
- Business purchases from vendors that sell consumer products
- Purchased items ‘returned’ to vendor without credit or refund
- Purchased items to be drop shipped or delivered to another location
Four main types of fraud

- **Asset Misappropriation:** Theft
- **Asset Misappropriation:** Embezzlement
- **Bribery / Corruption**
- **Financial Statement Misstatement**
Typical high risk areas: embezzlement

- Procurement and tendering
- Expense reimbursement
- Sales Commission / Invoicing
- Payroll
Embezzlement
Concealment of theft

Records altered to hide asset misappropriation, including for example:

• Purchases of overpriced services or materials
• Purchases of non-existing supplies
• Stock records manipulation – over statement, capitalization, inventory write-offs into consumption (*example of management fraud*)
• False documents used to obtain loans or payments
• Insurance claims
• Internet-banking and misuse of credit cards (also theft)
• Receivables write offs
• Changes in aging of receivables
• Capitalizing expenses (*example of management fraud*)
Other methods of embezzlement

- Receivables paid into private bank account
- Unsupported consulting / marketing / intermediary services
- Cash sales not recorded in the accounting records (skimming)
- Theft and concealment by repayment of shortly due receivables (lapping)
- Mischaracterised expenses, falsified travel requests
- Ghost employees: wages and salaries
- Internet-banking to an improper recipient
- Credit card fraud (often same as expense fraud)
- False returns and reclamations
- False incentive scheme claims
E.g. Commission or bonus schemes

**Description**
- Falsified figures
- Inflated sales made (false orders or invoices, altered prices, etc)
- Higher rates of commission

**Red Flags**
- No segregation of duties
- High degree of uncollected sales (e.g. by salesman)
- Significant change in commission earned (compared to other salesmen)
- Front loading or timing manipulation to beat targets
- Leads recognised as sales
Real life example

Embezzlement by procurement and finance staff in collusion
• Procurement employee falsified tender documents based on a previous supplier contract. Finance employee accomplice inputted details and registered his own bank account in the financial system of the firm, linking it to the fake supplier contract.
• Employees created false invoices allegedly from ‘renewed’ supplier.
• After each transaction, made by firm to this supplier, the employees split the transferred amounts received into the account.
• Lessons: verify banking details, run reports across employee and supplier bank account details to uncover duplicates, delist all contract-end suppliers, contact independently all new suppliers

Source: www.hvg.hu
Other procurement red flags

Examples

- Weak controls: same employee can order, receive and approve payment for goods / services
- Unusual / unexplained high volume purchases from a particular supplier
- Replacement or repairs after unreasonably short time period
- Invoiced goods or services cannot be located or verified
- Only one or a few bidders respond to request for bids
- Splitting cost into separate categories in order to avoid review
- Specifications inconsistent with past similar procurements
- Procurement too specific/vague (allows only favoured contractor/unqualified contractor to bid)
- Winning bid just under the next lowest bid (collusion with employees)
- Bidder not listed in business or telephone directories
- Subsequent increase in price of contract by unjustified / inflated change order requests
- Complaints from internal product / service users (high rate of rejections, returns, etc)
- Close socialization with and acceptance of inappropriate gifts, travel or entertainment from vendor
Four main types of fraud

- Asset Misappropriation: Theft
- Asset Misappropriation: Embezzlement
- Bribery / Corruption
- Financial Statement Misstatement
Bribery and corruption

Off-the-books / undisclosed interests

Conflicts of interest
- Purchases schemes
- Sales schemes
- Other

Bribery
- Kickbacks
- Bid rigging
- Other

Economic extortion
Illegal gratuities
Four main types of fraud

- Asset Misappropriation: Theft
- Asset Misappropriation: Embezzlement
- Bribery / Corruption
- Financial Statement Misstatement
Fraudulent financial reporting

- Timing differences
- Fictitious revenues or assets
- Improper valuations
- Improper disclosures
Financial statements misrepresentation

• Revenue misrepresentation is the most frequent
• Usually executed around decision of top management
• Thin line between fraud and aggressive accounting
• Simply executed. E.g.
  ➢ Cut off transactions
  ➢ Channel stuffing
  ➢ Fictitious sales
  ➢ Overestimated percentage of completion on projects
  ➢ Circular inventory transactions, consignment stock
  ➢ Non-market value transactions (i.e. inflated related party transactions)
Occupational fraud detection and prevention
Initial Detection of Occupational Frauds

Organizations > 100 employees

- Tip: 43.5%
- Management Review: 12.5%
- Internal Audit: 18.5%
- By Accident: 5%
- Account Reconciliation: 4.5%
- Document Examination: 3%
- External Audit: 3%
- Other*: 10%

Organizations < 100 employees

- Tip: 29.5%
- Management Review: 14.5%
- Internal Audit: 12%
- By Accident: 7.5%
- Account Reconciliation: 8.5%
- Document Examination: 5.5%
- External Audit: 6.5%
- Other: 16%

SMEs

*Law enforcement notification, surveillance/monitoring, IT controls, confession
Fraud Prevention Controls

Range of possibilities (big and small entities)

- Cash security measures
- Physical security measures
- Human security/guard dog service
- Electronic security systems (alarms)
- CCTV
- Employee segregation of duties
- Rotation of personnel
- Mandatory vacations
- Transaction authorization protocols
- Information security/logical access controls, inc. regular review and update
- Dual authorization payment procedures
- Setting of accounting system privileges
- Regular account reconciliations and review
- Management review
- Code of conduct/Ethics policy
- Disciplinary process
- Anti-fraud policy
- Business IT security/social media policy
- Electronic transaction monitoring systems (i.e. monitoring out of hours access)
- Fraud training for managers / employees
Fraud Prevention Controls

Range of possibilities (big and small entities)

- Formal fraud risk assessments
- Internal Audit *(key perception tool)*
- External audit *(key perception tool)*
- Surprise reviews/audits *(key perception tool)*
- New employee/business partner due diligence
- Whistleblower hotline/other tip-off system
- Rewards for whistleblowers
- Employee support programme
- Zero tolerance
- Tone at the top

‘Tone at the top’ promotes ethical behaviour
Detection and prevention in procurement / tendering processes

Some detection methods

• Verify new banking details, addresses
• Compare to procurement employees details
• Interview losing suppliers
• On-line research / background checks
• Review for incomplete information
• Invoice not original (photocopy/fax)
• Amounts rounded off
• Item description in code only
• Invoice amounts altered
• Sequential invoicing from supplier
Key internal control risks
Smaller organizations more susceptible due to lack of controls

Business Objective – Risk - Control Objective – Control Activity

Business / Personal Objective
A statement of intent to achieve a specific target

Risk
Something which could impact our ability to meet our objective

Control Objective
A statement of purpose to mitigate a specific risk

Control Activity
Activity that reduces risk to ensure we meet our objective
Key internal control risks
Consider fraud risks as part of every new project e.g. Expenditure

<table>
<thead>
<tr>
<th>Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no formal policies and procedures in place regarding maintenance to the Master Vendor List, including address and bank details and the use of one-time vendors at the local entity</td>
</tr>
<tr>
<td>Inadequate controls exist to ensure payments are not made to inactive vendors / fictitious vendors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payments could be made to fictitious/inappropriate vendors. Improper payments/inappropriate could be made and concealed as payments to fictitious vendors.</td>
</tr>
</tbody>
</table>

| Control Objective |
| Supplier master file is maintained and reviewed to ensure completeness and accuracy: Changes (input, alterations and deletions) to the supplier master file are processed completely, accurately and timely. |

| Control Activities |
| New permanent suppliers / significant changes are approved by purchasing department in accordance with purchasing policy. Changes are logged and processed timely. Purchases with one time suppliers are approved within a staged approval process considering purchasing volume. Supplier master file is periodically reviewed by management for accuracy and ongoing pertinence. Recorded changes to the master file are compared to authorized source documents to ensure that they were input accurately. |
Final thoughts: what to do when you are the victim of fraud
Common mistakes made in investigations

- Fail to plan ... plan to fail
- Losing temper, letting emotions get involved - consider whether independence required
- Suspect everyone, until proven otherwise - trust can blind you to facts
- Be open to all options, don’t assume
- Don’t lose control over the information flow - things can be missed
- Consider who you need to interview, when and in what order
- Not assessing information as it appears
- Investigation scope too narrow or fixed on too small a period of time
- Dismissing people before investigation takes place
- Not aware of disclosure/evidence requirements, breaching the law
Questions?
CONTACT

CAYMAN ISLANDS
Governors Square | Building 6
23 Lime Tree Bay Avenue
PO Box 31237
Grand Cayman | KY1-1205
Cayman Islands

tel +1 345 947 4700
fax +1 345 946 6728

BERMUDA
Chancery Hall | 1st Floor
52 Reid Street | Hamilton | HM 12
PO Box 671 | HM CX
Bermuda

tel +1 441 292 0818
fax +1 441 292 0826

CYPRUS (CIS/CEE)
5 Amathountos Street
5th floor
Pirilides Building
Limassol
Cyprus

tel +357 25830769
fax +357 25368913

BRITISH VIRGIN ISLANDS (Eastern Caribbean)
Commerce House | 2nd Floor
181 Main Street | Road Town
PO Box 930 | Tortola | VG1110
British Virgin Islands

tel +1 284 393 1768
fax +1 284 494 7169

GUERNSEY
La Plaiderie Chambers | 3rd
Floor La Plaiderie | St Peter Port
GY1 1WG
Guernsey

tel +44 1481 711 211
fax +44 1481 710 244

NEW YORK
New York
57W 57th St. | 4th Fl.
New York NY 10019
USA

tel +1 646 416-7904
fax +1 646 349-5735

BAHAMAS
Caves Village | Bldg 6, Upstairs Office 1
Blake Road and West Bay Street
PO Box SP-64064 | Nassau
Bahamas

tel +1 242 327 1447
fax +1 242 327 3288

LONDON
31st Floor | 40 Bank Street
London
E14 5NR
United Kingdom

tel +44 1481 711 211
e: John.Skelton@KRys-Global.com

PHOENIX
3240 N.Delaware St.
Chandler
AZ 85225
USA

tel +1 408 696-7711
fax +1 480 257-8600

KRYs-Global.com