Fraud Prevention and Detection

2010

Jim Downing, Chief Compliance Officer
Cheevers & Company
Member CHX/FINRA/SIPC
Disclaimer:

The findings and conclusions in this presentation are those of the author and do not represent the views of Cheevers & Company, its employees, owners, or affiliates. Nothing in this handout or presentation constitutes legal advice.

References Used in this Presentation:

- 2008 Report to the Nation on Occupational Fraud and Abuse by the Association of Certified Fraud Examiners, Inc.
- Donald R. Cressey, *Other People’s Money* (Montclair: Patterson Smith, 1973)
About the Presenter

Jim Downing, Chief Compliance Officer
Jim Downing serves as Chief Compliance Officer for Cheevers & Company. He brings with him 10 years of experience in SRO regulation, compliance, securities law, finance/accounting and risk management. Prior to joining the firm, he was a Compliance Examiner at FINRA where he was selected for several special projects including the mutual fund breakpoint sweep. Following five years with FINRA, Jim joined SunGard Institutional Brokerage where he was a Compliance Officer overseeing the institutional trading desk. Jim played an integral role in the company’s international expansion. Jim has a Master of Science in Accounting from Roosevelt University and is also a Certified Fraud Examiner. Currently, Jim is enrolled in the Executive Juris Doctorate program at Taft Law School and is a member of the National Society of Compliance Professionals.

Jim maintains his Series 7, 24, 27, 53 & 63 registrations with FINRA.
Objectives of the Presentation

- Understand why fraud occurs
  - Commonalities and findings that identify factors existent in fraud
- Fraud Prevention
  - Employee and management awareness
  - Risk Analysis & Internal Controls
  - Essential Methods of Prevention
- Fraud Detection
  - Internal Fraud
  - External Fraud
  - Fraud detection techniques
- Q&A Session
Fraud Facts

Gender of Fraudster

- Female: 41%
- Male: 59%

Position of Fraudster

- Owner/Exec: 23%
- Manager: 37%
- Employee: 40%

Age of Fraudster

- <26: 5%
- 26-30: 8%
- 31-35: 13%
- 36-40: 16%
- 41-50: 36%
- 51-60: 19%
- >60: 4%

Data from ACFE 2008 Report to the Nation
Fraud Facts – 2008 ACFE Report to the Nation

- Estimated that U.S. organizations lose as much as 7% of their annual revenue to fraud (p. 4).
- Fraud schemes cost organizations a median loss of $175,000 (p. 4).
- More than one quarter of frauds uncovered involved losses of at least $1 million dollars (p. 4).
- 46.2% of fraud cases uncovered were found via a tip (p. 18).
- A “poor tone at the top” was identified 8.6% of the time as the primary internal control weakness observed by Certified Fraud Examiner’s (p. 43).

What is important to remember is that anyone can commit fraud. If you are interested in learning more information visit the ACFE website at www.acfe.com.
Why Fraud Occurs

Donald R. Cressey (1919-1987) a noted scholar of fraud hypothesized that a classic model existed for the fraud offender. This became known as the “Fraud Triangle.”
Each Leg Explained

Pressure - Generally constitutes a “non-shareable” problem. This problem can be financial because that is usually the solution, money. For example, the fraudster steals in order to fix the problem. The problem can also be non-financial. For example the fraudster steals from the company because they feel they are not paid enough or out of revenge.

Opportunity – This can be created from witnessing other employees behavior, a known lack of internal controls within the company, or from the knowledge that the fraudster is in a position that could violate the trust of the company. An employee usually needs technical skills to commit the offense (e.g. familiar with accounting system, etc).

Rationalization – This takes place prior to the fraud being committed and contributes significantly to the motivation. Initially, the fraudster does not consider himself as a “criminal.” Thus, there is a need to justify the acts prior to commission. Fraudsters usually rationalize their crimes in three ways: (1) the belief the act is essentially not criminal, (2) the act is justified, or (3) they are part of a general scheme in which they were not completely culpable.
Albrecht Study

Dr. Steve Albrecht, Keith R. Howe and Marshall B. Romney, conducted an analysis of 200+ frauds in the early 1980’s and then released a book titled *Deterring Fraud: The Internal Auditor’s Perspective*. The book presented a list of the top 10 traits of fraudsters and the top 10 traits of organizations environments that were present in the study. While the list is not meant to be all inclusive the findings provide insight into the reasons behind why the people commit the acts and the deficiencies present at the organizations in which they are committed.
Traits of a Fraudster

Top Ten traits of a Fraudster
1) Living beyond their means
2) An overwhelming desire for personal gain
3) High personal debt
4) A close association with customers (e.g. family, friends)
5) Feeling pay was not commensurate with responsibility
6) A “wheeler-dealer” attitude
7) Strong challenge to “beat the system”
8) Excessive gambling habits
9) Undue family or peer pressure
10) No recognition for job performance
Organizational Traits

Top Ten traits of organizations that enable fraud:
1) Placing too much trust in key employees
2) Lack of proper procedures for authorization of transactions
3) Inadequate disclosure of personal investments/incomes
4) No separation of authorization of transactions from the custody of related assets.
5) Lack of independent checks on performance
6) Inadequate attention to details
7) No separation of custody of assets from the accounting of those assets
8) No separation of duties between accounting functions
9) Lack of clear lines of authority and responsibility
10) Department is not frequently reviewed by internal auditors
Why Fraud Occurs: Managements Role

One of the key factors in why fraud occurs is a lack of a unified message by a company’s senior management. This can lead to deficiencies that actually enable and perpetuate fraud.

It is important that management communicate their message to the employees to ensure that everyone understands the “tone at the top.”

Effective means of communication are:
1) Training
2) Initial and annual certification by employees
3) Establishing policies and procedures
4) Providing resources where employees can locate the tone of management (e.g. an intranet site, procedures, handbooks)
Fraud Prevention - Awareness

Fraud prevention is essential in managing risk within an organization. Methods exist that are easy to implement and will assist an organization in limiting liability of loss from fraud. Some of these methods will be discussed in this presentation.

One of the most effective fraud prevention techniques is to make employees aware of fraud and the companies efforts to detect and prevent fraud. Organizations should make it known that they monitor for fraud in order to ensure that employees and management are aware of the fact that someone is watching.
Training employees about fraud is also important to create awareness. Training can be done internally or externally. New technologies also provide for training via web or phone.

What is essential to any training plan is that it is consistently carried out. Give employees ample time to schedule required training and inform them of penalties for non-compliance. Many vendors provide for training and offer programs to implement on an enterprise wide scale.

It is important to customize any training to your firm to be effective. “Cookie cutter” programs, while informational, can often prove to be ineffective.
Fraud Prevention – Internal controls

Often touted as one of the most important aspects of a fraud prevention program, the separation of duties is essential in reducing fraud within any organization. Each of the following duties should ideally be segregated:

- Cash receipts and cash counts
- Bank deposits and deposit receipt reconciliation
- Bank reconciliations and posting of deposits/cash
- Purchasing and vendor payment functions
- Payroll Preparation and disbursement
- Safeguarding of assets and disbursement of assets
Fraud Prevention – Internal Controls

Section 404 of the Sarbanes-Oxley ("SOX") Act requires a company’s internal controls to ensure that all transactions reflect the financial position of the firm. While some entities may not be held to SOX the tenet of clear financial reporting is a good goal. This can be done by:

- Ensuring that each transaction is **authorized** by an employee
- Ensuring each transaction is **reported** to the company and no “off book” transactions occur
- Ensuring that each transaction is accurately **recorded** in the company’s books and records.
Fraud Prevention – Risk Analysis

An organization has an obligation to identify risk as it pertains to every facet of its business. When identifying risk seek out the experts in each department of the organization and ask them their opinion on what risks they see in their respective area of the business. It is important to quantify risk in terms of probability and its effect on the business. Some organizations use a numbered scale or tier risks based on how effectively they can be mitigated.
Fraud Prevention – Risk Analysis

Risk Matrix:

<table>
<thead>
<tr>
<th></th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From this example an organization can categorize risks into probability and consequence. Once that has been done the risk will then be classified on a scale of red, yellow, or green. Green being a risk the firm is willing to take (or mitigate) and red being something that should be addressed immediately.
Fraud Prevention – Risk Analysis

Senior management should conduct risk analysis at least annually to ensure that any potential new risk is addressed. Once the analysis is completed steps should be taken to mitigate risk. Assigning key employees to “own” the risk of their department will help guarantee that preventative steps are being taken. Remember to document the process from beginning to end as an effective audit trail will provide very useful evidence to auditors and examiners.
Fraud Prevention Methods - Hotline

Having a “fraud hotline” is an excellent and inexpensive way to prevent fraud within your organization. Inform employees, vendors, customers, and possibly the public of its existence. The Association of Certified Fraud Examiners 2008 Report to the Nation noted that 46% of frauds were uncovered from tips received from employees, customers, vendors, and other sources. The cost of implementing a fraud hotline is generally minimal compared to the amount that could potentially be saved.

It is important to create procedures for investigating tips received. Make sure that a formal process is in place if a tip needs to be escalated to the organizations audit committee or senior management.
Fraud Prevention Methods - Technology

Numerous vendors provide software to assist organizations in managing risk and fraud. Software can be a powerful tool in today’s digital age and can produce real results when implemented. Consider using software to monitor:

- Internal/external communications (e.g. email)
- The organizations banking transaction
- Employees personal trading accounts to avoid possible insider trading liability
- Conduct background checks and due diligence on employees/vendors
Fraud Prevention Methods – Audit

Conducting audits is the only way to interact with employees, review actual documents, and let employees know the organization is proactive in fighting fraud. Use templates or checklists to ensure consistent methods are being used across the organization.

Utilize sampling to avoid “over reviewing” while onsite.

Focus on most risk intensive activities of firm.
Fraud Detection

Fraud detection techniques vary across industries and can be very complex. However, some types of detection techniques are universal and apply to almost every organization. This section will provide “high level” fraud detection techniques that are simple to implement and can possibly uncover fraud.

Fraud is an unfortunate reality in today’s business world. The Association of Certified Fraud Examiners (ACFE) 2008 Report to the Nation estimated that US Organizations lose as much as 7% of their annual revenue to fraud. Fraud is committed against organizations both internally and externally.
Internal Fraud Detection Techniques

Conducting a vendor analysis:

An easy way to spot fraud committed by internal employees is to cross-reference the addresses of the company’s vendors with the home addresses of the employees.

Any match should be closely scrutinized to ensure that a legitimate reason exists.
Internal Fraud Detection Techniques

Reconcile all bank accounts and close dormant accounts:

Companies often only look to the bottom line on bank statements and do not review for outstanding checks or other red flags (such as breaks in check sequence numbers). Also closing any dormant accounts will prevent an internal employee from misusing the company’s bank relationship to commit fraud.
Internal Fraud Detection Techniques

Mandatory vacations:

While this method seems rather odd it can often provide very useful insight into an employee’s job functions and could uncover any improprieties the employee is attempting to conceal.

It is important to do the employee’s job in their absence, as this will most likely uncover any impropriety.
External Fraud Detection Techniques

Conducting due diligence on every vendor, business partner, and third party that is associated with your company.

Often times company’s conduct background checks on their employee’s but fail to do any due diligence on their vendors or associated parties. Due diligence can uncover financial hardships, regulatory problems, or even criminal activity. The level of due diligence should be commensurate with the activity.
External Fraud Detection Techniques

Know your customer: While this may also be a regulatory requirement for your company, using certain methods can often detect fraud being committed against your organization.

Common red flags are: customer residence outside of the company’s area, the customer’s actions are inconsistent with the objectives of the account, and large cash deposits/withdrawals without any explanation.
External Fraud Detection Techniques

Implement controls to prevent social engineering. Social engineering is the act of manipulating people into performing acts or divulging confidential information. The fraudster is usually looking to obtain confidential or proprietary information about the company.

Implementing controls to report this type of activity can assist an organization in detecting whether they have fallen victim to this often used method of fraud.

Controls/Policies to implement include: document destruction, provision of data access, user ID and password management, visitor access, and use of mobile computers outside the company.
Fraud Detection – Uncover Red Flags

Fraud detection is a method of uncovering red flags. A red flag is an outlier during the normal course of business that could suggest that a problem exists. There are four basic methods to uncovering red flags that can be used at almost every organization:

1) Surprise audits
2) Use of exception reports
3) Complaints by clients/vendors
4) Financial analysis
Fraud Detection – Surprise Audits

A surprise audit is one of the most powerful weapons to detect fraud. The surprise visit can catch the fraudster off guard where as an announced visit gives a person time to conceal, or even destroy, important evidence. Some important tips to remember when conducting a surprise audit:

- May take longer
- Ensure office will be staffed/open
- Bring list of items to review
- Try not to be adversarial
Fraud Detection – Exception Reports

Whether from a bank, clearing firm, accounting system, trust provider, or internal system, exception reports play an important role in the detection of fraud.

They can also demonstrate to outside auditors that your organization takes a proactive approach to mitigating risk. In many cases, the exception report provider can even customize the process to find red flags that are unique to your business.

If a report is redundant, it can also be changed to reflect real outliers and not flag every transaction. Contact your counterparties to inquire about the exception reports available to you.
Fraud Detection - Complaints by clients/vendors

Having proper procedures in place for the reporting and reviewing of customer/vendor complaints is essential. Complaints assist in the detection of fraud because they uncover red flags that might go unnoticed. Important questions to ask yourself about your organization:

- Does your organization give customers/vendors the proper means to report complaints?
- Does it inform them of where they can report a tip? (e.g. 800 number or email)
- What are the procedures for collecting and reviewing complaints?
- Do you have training to help employees identify complaints?

Complaints often are responsible for uncovering some of the biggest frauds in history.
Fraud Detection – Financial Analysis

There are two common types of financial analysis used to detect fraud, vertical and horizontal. Vertical analysis measures the relationship between items on the balance sheet, income statement, or cash flow statement using percentages. Horizontal analysis measures the percentage change between financial statement items over a period of time (e.g. month to month).

<table>
<thead>
<tr>
<th>Asset</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Change</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td>$1,000</td>
<td>83%</td>
<td>$750</td>
<td>60%</td>
</tr>
<tr>
<td>A/R</td>
<td>$200</td>
<td>17%</td>
<td>$500</td>
<td>40%</td>
</tr>
<tr>
<td>Total</td>
<td>$1,200</td>
<td>100%</td>
<td>$1,250</td>
<td>100%</td>
</tr>
</tbody>
</table>

Change $50 4.2%
Fraud Resources

Assoc. Of Certified Fraud Examiners – www.acfe.com


National Consumer League Fraud Center – www.fraud.org

FBI White Collar Crime - www.fbi.gov/whitecollarcrime.htm

AICPA - http://fvs.aicpa.org/Resources/Antifraud+Forensic+Accounting/

Ethicsline (hotline provider) - http://www.ethicsline.com/

Auditnet - http://www.auditnet.org/

Internet Fraud - http://www.usa.gov/Citizen/Topics/Internet_Fraud.shtml
Questions?