Who Owns Fraud: Uniting Corporate Executives to Manage and Analyze Fraud and Corruption Risks

Monday
June 21, 2011

IIA – Dallas Fraud Conference
Discussion topics

► The current fraud and corruption risk landscape

► Framework for an anti-fraud and anti-bribery compliance program: Who owns fraud?

► Forensic analytics to find hidden money

► New analytics & research, not your traditional accounting tests or mind set

► Integrating analytics using financial accounting data
  ► Expense, payables & customer analysis
  ► Case examples
  ► Predictive modeling

► Integrating analytics using email and user documents
  ► Communications with government or high-risk parties
  ► Fraud Triangle Analytics
  ► Advanced text mining techniques to identify the who, what, when and why
The top strategic risks for business
(ranking from 2009 in brackets)

1. Regulation and compliance (2)
2. Access to credit (1)
3. Slow recovery or double-dip recession (3)
4. Managing talent (7)
5. Emerging markets (12)
6. Cost cutting (6)
7. Non-traditional entrants (5)
8. Radical greening (4)
9. Social acceptance and CSR (New)
10. Executing alliances and transactions (8)
Current environment
The perfect storm for fraud & business corruption

- **Lack of infrastructure and controls in many foreign countries**

- **Layoffs, unemployment and unease continue**

- **Personal retirement plans and market levels remain low**

- **Companies are decentralized which has an immediate effect on internal controls**

- **Breach of anti-bribery regulatory focus increased globally**

- **Budgets are decreasing. Companies and organizations are doing more with less.**

- **Largest government contracts**

- **Stressed and disaffected employees may have greater ability to rationalize improper actions**

- **Employees are working in countries with perception of bribery**
Who owns fraud?
Who owns fraud?
How to approach

► Define the roles and responsibilities associated with the proactive and reactive initiatives.

► Identify the importance of developing coordination with these initiatives.

► Identify gaps to assist the company in enhancing the tone and culture within an organization to proactively and reactively respond to fraud.
Who owns fraud? — The issue

“Many corporations have too many departments handling fraud with no coordinated efforts.”

-Jim Ratley, President of the Association of Certified Fraud Examiners

Many companies struggle to determine who will be responsible for managing fraud proactively and reactively within their organization.
The elements of an anti-fraud program—
Who does what with respect to proactive and reactive approaches to fraud?

Who Owns Fraud?
Having a Seat at the Table.
Components of an anti-fraud & corruption compliance program

Elements of a successful corporate anti-fraud, bribery and corruption program

Anti-fraud, bribery and corruption key activities

- Corporate compliance assessment
- Corporate compliance design
- Gap analysis
- Future state design session
- Discovery response planning
- Records and information management

- Who owns fraud?
  - Assign roles and responsibilities
  - Fraud and risk committee formulation
  - Customized training
  - Corporate governance
  - Design sessions
  - Corporate anti-fraud road map
  - FCPA / anti-bribery compliance assessments

- Fraud risk assessment
  - Targeted anti-fraud analytics
  - Anti-bribery and corruption analytics
  - M&A Due Diligence
  - 3rd Party Due Diligence
  - Vendor Risk profiling
  - Vendor Vetting
  - Level I, II, III background checks

- Investigations
- Fraud response planning
- Forensic data analytics
- Discovery and document review

Setting the Proper Tone
- Code of Ethics
- Fraud and Corruption Prevention Policies
- Communication and Training

Proactive
- Risk Assessment
- Controls Monitoring and Analytics

Reactive
- Incident Response Plan

Management Ownership and Involvement
How to conduct a fraud risk assessment

Survey(s)
- Create and deliver customized surveys to different levels of management and employees throughout the organization.
- Allows for a mechanism to capture employees' perception of fraud risks and overall tone and culture within an organization.
- Employee responses are anonymous and this typically allows for more candid response.
- Graphical analysis and sharing of results with management provide insight into unforeseen risks, potential fraud, or other concerns.

Interview(s)
- One-on-one interviews allow participants the opportunity to have focused discussions, share opinions, review facts, and generate consensus on key business risk in the organization.
- Sometimes participants feel more comfortable in a small setting to share potential fraud risks.

Facilitated Session(s)
- Effective facilitated workshop sessions allow participants the opportunity to have focused discussions, share opinions, review facts, and generate consensus on key business risk in the organization identified in the survey, interviews, or during these sessions.
- Prioritize risks inside the organization into “Heat Maps”
- Determine next steps such as data analytics and review of controls.
End result: Where are your risks? — Next steps

- Fraudulent Statement Schemes
- Corruption Schemes
- Misappropriation of Asset Schemes

Severity of Impact

Critical
Significant
Minor

Likelihood of Occurrence

Very Rare
Possible
Likely
What types of fraud are occurring?

Source: ACFE 2010 Report to the Nations On Occupational Fraud
How prevalent is corruption (and related FCPA) risks?

CORRUPTION PERCEPTIONS INDEX 2010 RESULTS
Forensic Analytics – Finding Hidden Money
Where to start? The Fraud Tree

Who’s monitoring corruption?

<table>
<thead>
<tr>
<th>Corruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicts of interest</td>
</tr>
<tr>
<td>Bribery and corruption/FCPA</td>
</tr>
<tr>
<td>Illegal gratuities</td>
</tr>
<tr>
<td>Bid-rigging/procurement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fraudulent statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue recognition</td>
</tr>
<tr>
<td>GAAP</td>
</tr>
<tr>
<td>Reserves</td>
</tr>
<tr>
<td>Non financial</td>
</tr>
</tbody>
</table>

Asset misappropriation

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash larceny</td>
</tr>
<tr>
<td>Theft of other assets – inventory/AR/fixed assets</td>
</tr>
<tr>
<td>Fake vendor</td>
</tr>
<tr>
<td>Payroll fraud</td>
</tr>
<tr>
<td>T&amp;E fraud</td>
</tr>
<tr>
<td>Theft of data</td>
</tr>
</tbody>
</table>

General focus of internal auditors

General focus of external auditors
Fraud Risk Areas to Consider
“Monster List” library of over 400 tests...

Asset Misappropriation
- Cash Disbursements
- General Ledger
- Materials Management & Inventory Control
- Purchase Order Management
- Salaries & Payroll
- Travel & Expenses
- Vendor Management
- Payment Cards

Corruption / FCPA
- Bid Rigging
- Conflicts of Interest
- Contract Compliance
- Kickbacks
- Government Customers
- Payments to Agents
- Gifts & Entertainment
- Customs Payments
- Petty Cash
- Charity Payments

Financial Statement
- Accounts Payable
- Account Receivable
- Deposits
- General Ledger
- Revenue Recognition / Procure to Pay
- Sales Analysis
- Expense vs. Capitalization
- Management overrides
- Reserves manipulation
Most popular rules-based tests
Common Areas of Interest

1. Payment stream analysis
   ► Altered invoices, goods not received, duplicate invoices, inflated prices, excess quantities purchased

2. Vendor master/employee master comparisons
   ► Fictitious vendors, vendor risk ranking, conflicts of interest

3. Employee expenses and P-card expenditures
   ► Over limits, unusual expenses, miscellaneous/sundry expenses

4. Payroll
   ► Ghost employees, unusual payments, no deductions/evaluations, direct deposit account analysis

5. Bribery & Corruption / FCPA
   ► Bid rigging, conflicts of interest, contract compliance, kickbacks, payments to outside consultants
## Find Hidden Money...

### Duplicative payment analysis

<table>
<thead>
<tr>
<th>Vendor ID</th>
<th>VendorName</th>
<th>DocDate</th>
<th>Amt</th>
<th>Street Address</th>
<th>Invoice Number</th>
<th>PostDate</th>
<th>Reference Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>209655</td>
<td>PREMIER FOGHORN COAL CO</td>
<td>5/27/2008</td>
<td>$69,392</td>
<td>250 ALLISON BLVD</td>
<td>A334555</td>
<td>7/14/2008</td>
<td>QUAL10096</td>
</tr>
<tr>
<td>211132</td>
<td>JIMMY'S COAL SALES CO INC</td>
<td>5/27/2008</td>
<td>$69,392</td>
<td>PO. BOX 2679</td>
<td>A567664</td>
<td>6/16/2008</td>
<td>QUAL10096</td>
</tr>
<tr>
<td>208791</td>
<td>THOMPSON PETROLEUM CORPORATION</td>
<td>1/2/2008</td>
<td>$33,083</td>
<td>2480 SOUTH CLARES AVENUE</td>
<td>48617</td>
<td>1/9/2008</td>
<td>990924</td>
</tr>
<tr>
<td>211131</td>
<td>SPRINT PETROLEUM CO LLC</td>
<td>1/2/2008</td>
<td>$33,083</td>
<td>600 S MAIN ST</td>
<td>45840-3295</td>
<td>1/17/2008</td>
<td>990924</td>
</tr>
<tr>
<td>202771</td>
<td>BILLARD SPAHR ANDREWS</td>
<td>5/30/2008</td>
<td>$20,684</td>
<td>699 13TH ST NIV, STE 1003S</td>
<td>5564321</td>
<td>12/18/2008</td>
<td>2008056295</td>
</tr>
<tr>
<td>220493</td>
<td>BILLARD SPAHR ANDREWS</td>
<td>5/30/2008</td>
<td>$20,684</td>
<td>125 MARKET ST. 51ST FL</td>
<td>5564321-34</td>
<td>6/20/2008</td>
<td>2008056295</td>
</tr>
<tr>
<td>210128</td>
<td>ASA PETROLEUM COMPANIES INC</td>
<td>2/15/2008</td>
<td>$5,367</td>
<td>28999 WICK RD</td>
<td>481456</td>
<td>2/25/2008</td>
<td>569960</td>
</tr>
<tr>
<td>221688</td>
<td>ASA PETROLEUM COS INC</td>
<td>2/15/2008</td>
<td>$5,367</td>
<td>28999 WICK RD</td>
<td>48145-A</td>
<td>11/21/2008</td>
<td>569960</td>
</tr>
<tr>
<td>200565</td>
<td>REAL ESTATE TEN INC</td>
<td>1/4/2008</td>
<td>$22,756</td>
<td>25801 NORTHWESTERN, STE 215</td>
<td>345466</td>
<td>1/17/2008</td>
<td>41932CM</td>
</tr>
</tbody>
</table>

**Similar names**

**Some with same address**
Vendor / Employee conflicts of interest

Vendor Master and Employee Master should not overlap.

Analysis of phone numbers and fuzzy address matches.

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>Employee Address</th>
<th>Home Phone</th>
<th>Vendor Name</th>
<th>Vendor Address</th>
<th>Phone</th>
<th>YTD Paid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bristol, Jim J</td>
<td>30 Dean Wells Ct</td>
<td>6394565886</td>
<td>STONE GRASS COMPANY LLC</td>
<td>30 DEAN WELLS COURT</td>
<td>6394565886</td>
<td>$980</td>
</tr>
<tr>
<td>Bunton, Susie F</td>
<td>600 N Church</td>
<td>6557833693</td>
<td>COLD CREEK MACHINE &amp; TOOL</td>
<td>600 NORTH CHURCH ST</td>
<td>6557833693</td>
<td>$2,507</td>
</tr>
<tr>
<td>Smith, Debra A</td>
<td>2180 Millhaven Court</td>
<td>3146539490</td>
<td>HAZELWOOD EAST GRADUATION</td>
<td>ATTN DEBRA SMITH 11300 DUNN</td>
<td>3146539490</td>
<td>$9,766</td>
</tr>
<tr>
<td>Fehrenbacher, Jimmy</td>
<td>2115 N 600TH ST</td>
<td>6187522791</td>
<td>FEHRENBACHER CARPENTRY</td>
<td>2705 NORTH 600TH ST</td>
<td>6187522791</td>
<td>$5,674</td>
</tr>
<tr>
<td>Slider, Kim E</td>
<td>2 Meppen Drive</td>
<td>3338429601</td>
<td>LAW OFFICE OF KIM E SLIDER</td>
<td>4 MEPPEN DRIVE</td>
<td>3338429601</td>
<td>$15,350</td>
</tr>
<tr>
<td>Lopinotis, Douglas S</td>
<td>1702 N. 17th</td>
<td>6182772146</td>
<td>LOPINOTIS COMMUNICATIONS IN</td>
<td>26 LISA LANE</td>
<td>6182772146</td>
<td>$700,000</td>
</tr>
<tr>
<td>Woodsmith, Michael G</td>
<td>1388 Jones Place</td>
<td>5735927709</td>
<td>MICHAEL GENE WOODSMITH</td>
<td>P O BOX 1233</td>
<td>5735927709</td>
<td>$55,780</td>
</tr>
<tr>
<td>Wright, Kipper D</td>
<td>2222 W. 9th</td>
<td>6362392289</td>
<td>CUB SCOUT Pack 444</td>
<td>ATTN KIPPER WRIGHT 2222 W 9TH</td>
<td>6362392289</td>
<td>$500</td>
</tr>
</tbody>
</table>
Not your traditional accounting tests or mind set
How is fraud and corruption detected?

Source: ACFE 2010 Report to the Nations On Occupational Fraud

48.5% by tip or accident
Forensic analytics maturity model
*Beyond traditional “rules-based” queries and analytics*

![Diagram showing the relationship between detection rate, false positive rate, structured data, and unstructured data. The chart illustrates the transition from traditional rules-based queries and analytics to predictive modeling, statistical analysis, and data visualization.](image)
How important is text?

JofA: What new or recent technologies are changing the way CPAs investigate fraud?

Wells: There are, of course, many software programs available to do traditional data analysis. Perhaps the most inventive up-and-coming fraud-detection method is the use of textual analytics. It is still being perfected, but in a pilot research project by the ACFE and Ernst & Young, we developed a comprehensive list of key words and phrases that appear in e-mails that might be indicative of fraud. Examples include “can’t make the numbers,” “override,” “fudge” and “get caught.” There are many more.

-Joe Wells
June 2010 Journal of Accountancy
Focus on the payment text descriptions
What if you saw these terms used as justification for payments to third parties?

Nobody calls it “bribe expense”

Facilitation pay
Pay on behalf of

Special commission
Handover fee

One time payment

Help fee
Pay per management

Commission to the customer
Volume contract facilitation

Incentive payment
Text mining in the cash disbursements journal
Identify potentially improper payments

► Perform Text Analytics on free text fields
► Conduct “term frequency” analysis for most occurring or unusual transaction descriptions
► Capture “concepts”

“Volume contract facilitation”
“release expense”
ABC Analytics: Text mining dash board interface linked to cash disbursements
Disbursements Analysis
Who paid what, when, when and why?
Travel and expense analysis

Who, what, where, why, how…
Integrating anti-fraud analytics using financial accounting data
Travel & expense analytics

Analytics include:

► Where are expenses occurring (country, state, city) by category?
► What is the expense for?
► How much?
► Who is submitting?
► Duplicate expenses
► Text mining & keyword search

Questions to ask:

► Are there patterns with respect to who executives entertained (state owned entities, PEPs and other government officials)?
► Are there patterns of inappropriate expenses (nightclubs, gift giving, etc.)?
► Are there bogus reimbursements to fund improper cash to executives so they could to entertain public officials?
Vendor cash disbursement, payment analytics

Analytics include:

► Vendor stratification and clustering by amount and over time
► Duplicative invoice testing
► Requestor / approver conflicts – fake invoices or ghost vendors
► Conflicts of interest – employee and vendor master comparison
► Text mining and keyword searching of suspicious payment descriptions
► Identify government vendors or payments in unusual foreign currencies

Questions to ask:

► Did executives have fake vendors on the vendor master linked to their home, friends, or personal bank accounts?
► Were there duplicative invoices being submitted to extract cash?
► Were executives overriding controls to extract cash for bribes?
► What are the nature of the vendors that certain executives approved?
Customer analytics

Analytics include:
► Customer stratification and clustering by amount and over time
► Free goods, credits and discount sales analysis/comparison to customers
► Conflicts of interest – employee and customer master comparison

Questions to ask:
► Are any customers getting favorable treatment from certain executives in terms of average sale price, discounts, credits, etc.?
► Are there customers related to certain executives that pose conflict of interest concerns? E.g., family members, same last name, same bank account, same address, etc.
Predictive modeling

**Challenge:** Analyze 400,000 transactions for suspected bribery payments per DOJ subpoena

1. Team reviewed 2,000 transactions from ledger data (text comments, amounts, dates, etc.)
   - Identified 400 suspicious and 1,600 non-suspicious entries


3. Applied model to remaining 398,000 additional transactions

4. Identified 14,000 new suspicious transactions
   - With confidence over 95% similar to “Is Suspicious”
   - Identified over $8 million in highly suspicious payments
   - Methodology accepted by the DOJ for this case
These three variables were the highest drivers of suspicious transactions. Client should focus resources on monitoring efforts for the three leading drivers, which accounts for 80% of the predictive value.

These variables were less important when predicting suspicious transactions.

Perform Variable Analysis

Cumulative Distribution Analysis
Profile of Suspicious Transactions
Integrating anti-bribery analytics using email and user documents
Email and document analysis

Analytics include:

► Targeted keyword search around high-risk projects, customers, etc.
► Keyword search in local language
► Domain name searches and review of non company email – @gmail.com, @yahoo.com, etc.

Questions to ask:

► Are there improper relationships with government officials, customers, inspectors?
► Are there discussions about improper entertainment?
► Are there discussions asking for “special treatment”, “special payment”, etc.?
Email and document analysis

Analytics include:

► Targeted keyword search
► Social network analysis (who’s talking to whom)
► Date frequency analysis (who said what, when)
► Fraud Triangle Analytics (linking email to components of the Fraud Triangle)

Questions to ask:

► Are there improper relationships with employees?
► Are there improper relationships with government officials/inspectors?
► Are there improper relationships with customers or vendors?
The Fraud Triangle¹
Applying the theory to email communications

1. Donald R. Cressey’s “Fraud Triangle”; Incentive/Pressure, Opportunity and Rationalization are present when fraud exists.
Interactive Email Analysis Dashboard

Fraud Triangle Analytics to identify top individuals using words of “incentive/pressure”, “opportunity” and “rationalization”
### Advanced E-mail Analytics – text mining

<table>
<thead>
<tr>
<th>WHO</th>
<th>WHAT</th>
<th>WHEN</th>
<th>WHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Networking</td>
<td>Concept Clustering and Keywords</td>
<td>Communication Over Time</td>
<td>Sentiment Analysis</td>
</tr>
</tbody>
</table>

**“Who is talking to whom?”**

- People-to-people analysis
- Entity-to-entity analysis
- Map communication lines to organization chart

**“About what?”**

- Top words mentioned
- Key concepts / topics
- Top or unusual dollar amounts
- Sensitive words / phrases

**“Over which time period?”**

- When communications occur
- Communication spikes around key business events

**“How do they feel?”**

- Positive vs. Negative Sentiment
- Top 10 angry or negative emails
- Customer survey analysis
- Employee survey analysis
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Example use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor proximity</td>
<td>Multi-dimensional analysis of closeness of relationships</td>
<td>Accurate identification of associates of a bad actor</td>
</tr>
<tr>
<td>Actor centrality</td>
<td>Determination of most important actors in a network</td>
<td>Rapid identification of an organization’s influencers</td>
</tr>
<tr>
<td>Anomalous communication density</td>
<td>Detection of individual instances of a topic or workflow process attracting an unusual degree of attention</td>
<td>Identification of occurrences of non-compliance with standard processes</td>
</tr>
<tr>
<td>Anomalous ad hoc workflow sequences</td>
<td>Detection of steps that are out of order compared with the norm</td>
<td>Identification of occurrences of non-compliance with standard processes</td>
</tr>
<tr>
<td>Stressful Topics</td>
<td>Identification of topics evoking unusual levels of stress in discussions among a group of actors</td>
<td>Determination of processes that cause friction</td>
</tr>
<tr>
<td>Deletion analysis</td>
<td>Comparison of deletion patterns among related actors</td>
<td>Detection of potentially conspiratorial behavior</td>
</tr>
<tr>
<td>Textblock analysis</td>
<td>Strings of text DNA</td>
<td>Patterns of influence, data leakage</td>
</tr>
<tr>
<td>Social network shift</td>
<td>Topic-filtered social network</td>
<td>Determination of who participates in, and who is excluded from, what types of conversation</td>
</tr>
<tr>
<td>Document lifecycle</td>
<td>Reconstruction of document edit history</td>
<td>Detection of unusual patterns of activity, non-compliance</td>
</tr>
<tr>
<td>Spread of information</td>
<td>Time-lapse spread of topic or textblock</td>
<td>Determination of data leak sources</td>
</tr>
<tr>
<td>Mindshare</td>
<td>Apparent focus of an actor’s attention</td>
<td>Determination of likely extent of actor’s knowledge of a given issue</td>
</tr>
</tbody>
</table>
Integrating investigative skills with both email and financial accounting information (an example)

1. A suspicious vendor is identified in the payables data.
2. That vendor name is searched in the email communications to gather the full context.
3. Email and transactional data is discussed with interviewee to support confession.
Questions & Discussions

Daniel Torpey, CPA
Partner
daniel.torpey@ey.com
214-969-8373

Vincent Walden, CFE, CPA
Partner
vincent.walden@ey.com
214-754-3941