Trends in the Detection of Fraud Schemes

Initial Detection of Occupational Frauds

Detection Method

- Tip
- Internal Audit
- Management Review
- By Accident
- Account Reconciliation
- Other
- Document Examination
- External Audit
- Notified by Law Enforcement
- Surveillance/Monitoring
- IT Controls
- Confession

Percent of Cases

- 2016
- 2014
- 2012
Trends in the Detection of Fraud Schemes

Detection Method by Scheme Type

- **Tip**
  - Asset Misappropriation: 37.3%
  - Corruption: 31.8%
  - Financial Statement Fraud: 46.0%
- **Internal Audit**
  - Asset Misappropriation: 16.7%
  - Corruption: 16.5%
  - Financial Statement Fraud: 18.8%
- **Management Review**
  - Asset Misappropriation: 14.1%
  - Corruption: 14.8%
- **Account Reconciliation**
  - Asset Misappropriation: 6.3%
  - Corruption: 4.0%
- **By Accident**
  - Asset Misappropriation: 6.2%
  - Corruption: 4.5%
- **Other**
  - Asset Misappropriation: 5.4%
  - Corruption: 6.5%
  - Financial Statement Fraud: 9.4%
- **External Audit**
  - Asset Misappropriation: 3.7%
  - Corruption: 3.4%
  - Financial Statement Fraud: 6.7%
- **Document Examination**
  - Asset Misappropriation: 3.5%
  - Corruption: 3.5%
- **Notified by Law Enforcement**
  - Asset Misappropriation: 2.2%
  - Corruption: 2.2%
  - Financial Statement Fraud: 3.4%
- **Surveillance/Monitoring**
  - Asset Misappropriation: 1.9%
  - Corruption: 1.9%
  - Financial Statement Fraud: 4.0%
- **IT Controls**
  - Asset Misappropriation: 1.4%
  - Corruption: 1.1%
  - Financial Statement Fraud: 0.4%
- **Confession**
  - Asset Misappropriation: 1.2%
  - Corruption: 0.6%
  - Financial Statement Fraud: 3.1%
Detection of Fraud Schemes

- Detection methods varied substantially between small organizations. The starkest variation occurred with tips.

- Internal audit was the detection method for 12% of cases at small organizations but 18.6% at larger organizations.

- One possible explanation for these disparities is that the controls and procedures an organization has in place affect how fraud schemes are caught.

- In place of tips, small organizations tend to detect more frauds through management review, account reconciliation, accident, external audit, and document examination.
Median Losses by Region

- **Canada**: $154,000
- **United States**: $120,000
- **Latin America and the Caribbean**: $174,000
- **Western Europe**: $263,000
- **Eastern Europe and Western/Central Asia**: $200,000
- **Middle East and North Africa**: $275,000
- **Southern Asia**: $100,000
- **Sub-Saharan Africa**: $143,000
- **Asia-Pacific**: $245,000
Fraud Schemes by Region

United States

**MEDIAN LOSS:** $120,000  **CASES:** 1,038
Fraud Schemes by Region

Latin America and The Caribbean

MEDIAN LOSS: $174,000  CASES: 112
Fraud Schemes by Region

Asia-Pacific

**MEDIAN LOSS:** $245,000  **CASES:** 221
Fraud Schemes by Region

**Middle East and North Africa**

**Median Loss:** $275,000  **Cases:** 79
Median Loss per Fraud Scheme

$125,000
ASSET MISAPPROPRIATION

$200,000
CORRUPTION

$975,000
FINANCIAL STATEMENT FRAUD
Asset Misappropriation Schemes

Frequency and Median Loss of Asset Misappropriation Sub-Schemes

- Check Tampering
- Cash Larceny
- Payroll
- Skimming
- Expense Reimbursements
- Non-Cash
- Register Disbursements
- Cash on Hand
- Billing

© 2016 Association of Certified Fraud Examiners, Inc. All rights reserved
Companies are taking a strong, proactive stance in investing their FDA spend

According to the Association of Certified Fraud Examiners’ most current Report to the Nations on Occupational Fraud and Abuse, those companies with proactive data analytics in place saw a cost per fraud incident that was 59.7% lower (roughly US$100,000 lower per incident) than the cost for those companies not using proactive data analytics – more than any other control listed in the survey.

As we look toward COSO guidance around conducting fraud risk assessments as part of an effective internal controls framework, we will see a strong emphasis on the use of forensic data analytics.

63% of respondents
Spend at least half of their FDA investment on proactive initiative
## EY survey approach and participant profile

<table>
<thead>
<tr>
<th>Job title</th>
<th>Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of internal audit/CRO</td>
<td>192</td>
</tr>
<tr>
<td>Other audit/risk</td>
<td>81</td>
</tr>
<tr>
<td>Other finance</td>
<td>51</td>
</tr>
<tr>
<td>Head of compliance</td>
<td>61</td>
</tr>
<tr>
<td>CFO/FD</td>
<td>68</td>
</tr>
<tr>
<td>Head of legal</td>
<td>34</td>
</tr>
<tr>
<td>Financial controller</td>
<td>58</td>
</tr>
<tr>
<td>CEO/COO/CIO</td>
<td>28</td>
</tr>
<tr>
<td>Head of business unit/division</td>
<td>16</td>
</tr>
<tr>
<td>Head of investigations</td>
<td>14</td>
</tr>
<tr>
<td>Head of security</td>
<td>17</td>
</tr>
<tr>
<td>Company secretary</td>
<td>5</td>
</tr>
<tr>
<td>Other management staff</td>
<td>40</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>162</td>
</tr>
<tr>
<td>Consumer products/Retail/Wholesale</td>
<td>149</td>
</tr>
<tr>
<td>Life sciences</td>
<td>59</td>
</tr>
<tr>
<td>Oil and gas</td>
<td>62</td>
</tr>
<tr>
<td>Power and utilities</td>
<td>41</td>
</tr>
<tr>
<td>Transportation</td>
<td>24</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>62</td>
</tr>
<tr>
<td>Mining</td>
<td>27</td>
</tr>
<tr>
<td>Technology, communications and</td>
<td>77</td>
</tr>
<tr>
<td>entertainment</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
</tr>
</tbody>
</table>
Key findings: current state of FDA adoption

Current and emerging risks driving demand
- The fastest-growing fraud risk is cyber breach or insider threat, with 62% of respondents reporting increased levels of concern in this area.

A maturing FDA landscape
- Three out of five respondents plan to increase their spend on forensic data analytics (FDA) over the next two years.
- 63% are investing at least half of their FDA spend on proactive monitoring activities.
- Technology maturity is also growing. The use of visualization tools has doubled since the 2014 survey.
- Respondents conducting FDA completely in-house increased from 45% two years ago to 67%.
- Organizations are not recognizing the full spectrum of value FDA can deliver, specifically with respect to cost savings.
Current and emerging risks driving demand

“At the SEC, we have made great strides in leveraging data and technology to detect and pursue misconduct. In the enforcement arena, the Commission is using data analytics to help identify wrongdoers and conduct streamlined investigations to optimize our resources.”

– Chair Mary Jo White, opening remarks at the 21st Annual International Institute for Securities Enforcement and Market Oversight, 2 November 2015
FDA demand is also driven by increasing government and public scrutiny of fraud risk.

Q. What are the main reasons that you are planning to increase your investment in FDA capabilities?

Base: Respondents who plan to increase investment in FDA (405)

**Multiple answers allowed, may exceed 100%**

- Increased regulatory scrutiny: 43%
- Response to growing cybercrime risks: 53%
- Increased risk of fraud in emerging markets: 32%
- Pressure from the board or management team: 31%
- Seeking greater cost efficiency in the fraud risk management process: 30%
- Recent fraud risk assessment findings in the organization: 26%
- Need for more robust third-party due diligence: 25%
- Increasing merger and acquisition activities: 13%
- Increased calls to your ‘whistle-blower line’: 9%
- Other main reasons: 4%
Worldwide regulatory enforcement is driving the sense of urgency by C-suite respondents

► The SEC’s Financial Reporting and Audit Task Force is now deploying cutting-edge FDA tools to mine data for fraud.

► Regulators in the UK, Germany, Italy and France, among others, have been involved in major enforcement actions.

► In Asia, prosecutions for corruption are increasingly frequent, with China leading the way.

► EU and Japan regulators are teaming with their US counterparts on cartel investigations.
Cyber breach or insider threat is perceived as the fastest-growing fraud risk

Q. Over the past two years, how has the level of concern about each risk area changed in your organization?
Base: All respondents (665)

The “Don’t know” percentages have been omitted to allow better comparison among the responses given.
### Perceived risks by industry - the percentage of respondents who have seen the increased level of risks

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cyber breach or insider threat</th>
<th>Bribery and corruption risk</th>
<th>Internal fraud (travel and entertainment abuse, collusion, etc.)</th>
<th>Capital projects risk</th>
<th>Merger and acquisition risk</th>
<th>Money laundering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td><strong>74%</strong></td>
<td>50%</td>
<td>47%</td>
<td>24%</td>
<td>25%</td>
<td>46%</td>
</tr>
<tr>
<td>Life sciences</td>
<td><strong>63%</strong></td>
<td>49%</td>
<td>49%</td>
<td>42%</td>
<td>29%</td>
<td>19%</td>
</tr>
<tr>
<td>Transportation</td>
<td><strong>46%</strong></td>
<td>46%</td>
<td>38%</td>
<td>38%</td>
<td>33%</td>
<td>29%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td><strong>48%</strong></td>
<td>35%</td>
<td>32%</td>
<td>32%</td>
<td>24%</td>
<td>18%</td>
</tr>
<tr>
<td>Consumer products, retail and wholesale</td>
<td><strong>64%</strong></td>
<td>38%</td>
<td>42%</td>
<td>35%</td>
<td>21%</td>
<td>23%</td>
</tr>
<tr>
<td>Technology, communications and entertainment</td>
<td><strong>55%</strong></td>
<td>48%</td>
<td>49%</td>
<td>34%</td>
<td>29%</td>
<td>17%</td>
</tr>
<tr>
<td>Oil and gas</td>
<td><strong>61%</strong></td>
<td>52%</td>
<td>35%</td>
<td>35%</td>
<td>37%</td>
<td>19%</td>
</tr>
<tr>
<td>Mining</td>
<td><strong>52%</strong></td>
<td>37%</td>
<td>30%</td>
<td>30%</td>
<td>33%</td>
<td>11%</td>
</tr>
<tr>
<td>Power and utilities</td>
<td><strong>56%</strong></td>
<td>41%</td>
<td>34%</td>
<td>46%</td>
<td>44%</td>
<td>10%</td>
</tr>
</tbody>
</table>
FDA deployment: what are the key hurdles?
Key challenges: making the business case

Discrepancy between practice and perception

Q. To what extent do you agree that “We need to improve management’s awareness of the benefits of FDA in the company’s anti-fraud program”?
Base: All respondents (665)
The “Don’t know” percentages have been omitted to allow better comparison among the responses given.

74% of C-suite respondents

“We need to do more to improve our current anti-fraud procedures, including the use of FDA tools.”

Q. To what extent do you agree that “We need to improve management’s awareness of the benefits of FDA in the company’s anti-fraud program”?
Base: All respondents (665)
The “Don’t know” percentages have been omitted to allow better comparison among the responses given.
Key challenges: building teams with the right skills

Successful deployment requires three distinct skill sets:

► **Technical skills** – to understand the organization’s systems and advise on acquiring additional technology

► **Domain knowledge** – familiarity with the relevant risk areas in the business and the ability to interpret analytics results in the context of the organization

► **Data analytics (e.g., data science) expertise** – mathematical, computer science and business intelligence techniques, such as pattern recognition, statistical analysis, query design and data visualization

According to Gartner, the need for data scientists is growing at about three times that for statisticians and business intelligence analysts, and there is an anticipated talent shortage of 100,000 or more analytics personnel through 2020.

Don’t forget the human element of your FDA program

“In 39% of leading analytics organizations – versus 12% of the rest – analytics skills are recognized, effective, efficient, monitored and clearly used to support decisions. More than one-third of the top 10% also have well-defined competencies for each role and level, along with robust training programs that address potential skills shortages.”

EY and Forbes Insights, Data and Analytics Impact Index: don’t forget the human element of analytics, 2015.
Key challenges: deploying the right technology

► Respondents continue to rate “challenges in combining data sources” as the top issue to overcome when implementing FDA.
  ► Building data sets that talk to one another is the first step to successful analytics.
► One key obstacle to moving to more advanced tools appears to be the lack of funding.
► However, analytics technology has improved, making deployment and accessibility easier.
  ► More “self-service” applications are available via cloud that require less customization to implement.
  ► Significant improvements in computing power and scalability (i.e., Hadoop) combined with ever-decreasing storage costs make the use of FDA more cost effective.
What Does Good Look Like?
Intentionally left blank for distribution purposes
Key findings: what does good look like?

Use advanced technology
► In almost every circumstance, those companies using more sophisticated analytics, beyond basic spreadsheet-type, rules-driven tests, report better fraud detection in less time.

Analyze large data volumes
► We have observed a positive correlation between the use of large data volumes (over 10 million records) and achieving positive results of FDA implementation.

Analyze a wide variety of data
► Our survey findings indicate that respondents who have reported positive results from using FDA are using a wider variety of data sources.
Commonalities among those with successful results

Q. What tools do you utilize in managing fraud risks?

<table>
<thead>
<tr>
<th>Tool</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visualization</td>
<td>29%</td>
</tr>
<tr>
<td>Social media</td>
<td>30%</td>
</tr>
<tr>
<td>Statistical analysis</td>
<td>7%</td>
</tr>
</tbody>
</table>

Q. What data volume (in records) do you typically work with in your FDA tasks?

<table>
<thead>
<tr>
<th>Data Volume</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 1m</td>
<td>53%</td>
</tr>
<tr>
<td>Between 1m and 10m</td>
<td>57%</td>
</tr>
<tr>
<td>More than 10m</td>
<td>79%</td>
</tr>
</tbody>
</table>

Q. Which of the above unstructured data sources does your organization use to analyze fraud risks?

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic communication</td>
<td>67%</td>
</tr>
<tr>
<td>Free text payment descriptions in accounting data</td>
<td>55%</td>
</tr>
<tr>
<td>News feeds or external data sources</td>
<td>57%</td>
</tr>
<tr>
<td>Social media</td>
<td>49%</td>
</tr>
<tr>
<td>Customer call or meeting notes</td>
<td>46%</td>
</tr>
<tr>
<td>Network system or server information</td>
<td>71%</td>
</tr>
</tbody>
</table>

Q. Of your annual spend on preventing and detecting fraud risks, what percentage is on FDA specifically?

<table>
<thead>
<tr>
<th>Spend Percentage</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2%</td>
<td>14%</td>
</tr>
<tr>
<td>7%</td>
<td>20%</td>
</tr>
<tr>
<td>11%</td>
<td>20%</td>
</tr>
<tr>
<td>19%</td>
<td>29%</td>
</tr>
</tbody>
</table>

Q. Of your annual spend on preventing and detecting fraud risks, what percentage is on FDA specifically?

<table>
<thead>
<tr>
<th>Invest more of total anti-fraud spend in FDA</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invest more of total anti-fraud spend in FDA</td>
<td>33%</td>
</tr>
</tbody>
</table>

Base: Among all respondents (665), 56% (370) agree and 21% (140) disagree that “We currently get positive results from the FDA tools that we use.”
Detection of Fraud Schemes

Source: ACFE Report to the Nations 2016
Fraud Trends and Investigations
Mitigating Fraud

Approaches used by companies to minimize and mitigate potential or existing fraud:

- **Fraud Prevention**
  - Setting strong tone at the top
  - Implementing policies and procedures in order to prevent fraud from occurring
  - Developing fraud training and awareness
  - Establishing strong Internal controls

- **Fraud Detection**
  - Internal controls
  - Hotline

- **Fraud Response**
  - Internal Investigation
  - Independent Investigation
Fraud Response
Investigating Fraud Allegations

► Overview
► Components of an Anti-Fraud Program – Fraud Response
► Response Protocols
► Types of Investigations
► Reporting the Results
► Investigation Challenges
Intentionally left blank for distribution purposes
Response Protocols

► Receive the allegation
► Understand the nature of the allegation
  ► Determine whether it involves a potential violation of laws, rules, or company policy (establish privileged as appropriate)
  ► Ask the following questions:
    ► What is the source of the allegation
    ► When and where did the events occur and over what period of time
    ► What evidence may exist
    ► Who may be involved
    ► Who is likely to have relevant knowledge or information
► Determine the appropriate course of action
  ► Consult the necessary resources to determine the “next steps”
  ► Assemble the team to conduct the investigation
  ► Preserve the data, especially electronic data
Types of Investigations - Internal

- Conducted at the direction of management and the Company’s in-house or outside counsel
- Initiated by management or prompted by an external event
- Management should do all that it can to prepare an informed defense to existing or anticipated allegations of wrongdoing
Types of Investigations - Independent

► Conducted at the direction of a committee of the Board of Directors (e.g. Audit Committee or Special Committee) with outside counsel

► Why an independent investigation?
  ► Consistent with focus of Sarbanes-Oxley
  ► Credibility with regulators – i.e. SEC and DOJ
  ► Expectation of external auditor
  ► Expectation of regulators
Investigation Challenges

► Maintaining Privilege while keeping all interested parties informed
► Electronic discovery
► Interview process
► Management does not respect the investigation
► Auditors do not accept the results
► Regulators are not satisfied with results
► What to do with the results?
Reporting to Authorities

► **Self-report**
  ► Proactively cooperate and substantially assist in investigations
    ► Examples: self-reporting potential violations, translate key documents, produce witnesses from foreign jurisdictions, undertake remedial actions, effective compliance and ethics program
  ► Possibly avoid appointment of a monitor
  ► Reduction in enforcement penalties
    ► Receive credits

► **Not to self-report**
  ► Wait and see
    ► Limited credits received when compared to voluntary self-disclosure
  ► Harsher penalties
Fraud in the News

► PTC Inc.
  ► February 2016: Two China units of the Massachusetts software company entered into a non-prosecution agreement and paid a $14.5 million criminal penalty to resolve a DOJ investigation into payments for recreational travel by Chinese government officials. PTC China didn't receive voluntary disclosure credit or full cooperation credit, the DOJ said.

► PJT Partners
  ► March 2016: Andrew Caspersen, a partner in a New York investment bank, was arrested for trying to defraud investors of more than $95 million. "Caspersen allegedly…creating fake email addresses, setting up misleading domain names, and inventing fictional financiers.” PJT Partners referred the matter to federal prosecutors after learning facts suggesting improper behavior.

► Braid Group (Holdings) Limited
  ► April 2016: Braid's internal investigation revealed bribery in connection with two Braid UK freight forwarding contracts in 2012. During the investigation, Braid discovered separate bribery offenses regarding a second customer and self reported the offenses to the Crown Office. The company admitted that it violated Sections 1 (bribery) and 7 (failure to prevent bribery) of the Bribery Act.
Thank You

Questions?
Contact Information

► Kathleen Chu, Senior Manager
  Los Angeles Office
  Email: Kathleen.Chu@ey.com
  Office: 1 (213) 977-3665

► Jonathan Huynh, Senior Manager
  Los Angeles Office
  Email: Jonathan.Huynh@ey.com
  Office: 1 (213) 977-1546
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2015 Ernst & Young LLP.
All Rights Reserved.

ED none

www.ey.com