Dealing with Fraud in a High-Tech Age

Wednesday May 25, 2016 | 8:30am – 10:10am | 2 CPE

Shauna Woody-Coussens, Managing Director – Forensics & Valuation Services, BKD
Brian Sanvidge, Principal - National Forensic Litigation and Valuation Services, Baker Tilly
Anne Harty, Chief Financial Officer, City of Rock Hill, SC
TRENDS IN OCCUPATIONAL FRAUD

$6.3 BILLION IN TOTAL LOSSES

23% OF CASES CAUSED LOSSES OF $1 MILLION OR MORE

$150,000 MEDIAN LOSS PER CASE
2nd Most Targeted Industry

Median loss for government entities is $133,000
# MOST EFFECTIVE ANTI-FRAUD CONTROL

**Figure 59: Median Loss Based on Presence of Anti-Fraud Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Percent of Cases</th>
<th>Control in Place</th>
<th>Control Not in Place</th>
<th>Percent Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Data Monitoring/Analysis</td>
<td>36.7%</td>
<td>$92,000</td>
<td>$200,000</td>
<td>54.0%</td>
</tr>
<tr>
<td>Management Review</td>
<td>64.7%</td>
<td>$100,000</td>
<td>$200,000</td>
<td>50.0%</td>
</tr>
<tr>
<td>Hotline</td>
<td>60.1%</td>
<td>$100,000</td>
<td>$200,000</td>
<td>50.0%</td>
</tr>
<tr>
<td>Management Certification of Financial Statements</td>
<td>71.9%</td>
<td>$104,000</td>
<td>$205,000</td>
<td>49.3%</td>
</tr>
<tr>
<td>Surprise Audits</td>
<td>37.8%</td>
<td>$100,000</td>
<td>$195,000</td>
<td>48.7%</td>
</tr>
<tr>
<td>Dedicated Fraud Department, Function, or Team</td>
<td>41.2%</td>
<td>$100,000</td>
<td>$192,000</td>
<td>47.9%</td>
</tr>
<tr>
<td>Job Rotation/Mandatory Vocation</td>
<td>19.4%</td>
<td>$89,000</td>
<td>$170,000</td>
<td>47.6%</td>
</tr>
<tr>
<td>External Audit of Internal Controls over Financial Reporting</td>
<td>67.6%</td>
<td>$105,000</td>
<td>$200,000</td>
<td>47.5%</td>
</tr>
<tr>
<td>Fraud Training for Managers/Executives</td>
<td>51.3%</td>
<td>$100,000</td>
<td>$190,000</td>
<td>47.4%</td>
</tr>
<tr>
<td>Fraud Training for Employees</td>
<td>51.6%</td>
<td>$100,000</td>
<td>$186,000</td>
<td>46.8%</td>
</tr>
<tr>
<td>Formal Fraud Risk Assessments</td>
<td>39.3%</td>
<td>$100,000</td>
<td>$187,000</td>
<td>46.5%</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>56.1%</td>
<td>$100,000</td>
<td>$183,000</td>
<td>45.4%</td>
</tr>
<tr>
<td>Anti-Fraud Policy</td>
<td>49.6%</td>
<td>$100,000</td>
<td>$175,000</td>
<td>42.9%</td>
</tr>
<tr>
<td>Internal Audit Department</td>
<td>73.7%</td>
<td>$123,000</td>
<td>$215,000</td>
<td>42.8%</td>
</tr>
<tr>
<td>Code of Conduct</td>
<td>81.1%</td>
<td>$120,000</td>
<td>$200,000</td>
<td>40.0%</td>
</tr>
<tr>
<td>Rewards for Whistleblowers</td>
<td>12.1%</td>
<td>$100,000</td>
<td>$163,000</td>
<td>38.7%</td>
</tr>
<tr>
<td>Independent Audit Committee</td>
<td>62.5%</td>
<td>$114,000</td>
<td>$180,000</td>
<td>36.7%</td>
</tr>
<tr>
<td>External Audit of Financial Statements</td>
<td>81.7%</td>
<td>$150,000</td>
<td>$175,000</td>
<td>14.3%</td>
</tr>
</tbody>
</table>
DEFINITION OF DATA ANALYTICS

...processes & activities designed to obtain & evaluate data to extract useful information and answer strategic questions...
DATA ANALYTICS

// Answer questions through use of analytical software
  // As simple as Excel
  // Filter
  // Sort
  // As complex as you want to make it
  // ACL
  // IDEA
  // Sequel
DATA ANALYTICS – COMMON CHALLENGES

// Existence of useful data
// Data quality
// Ownership of data
// Organizational culture
// Lack of expertise & personnel
// Volume of data available
APPLICATIONS IN GOVERNMENT SECTOR
# FRAUD SCHEMES BY INDUSTRY

**Figure 45: Frequency of Schemes Based on Industry**

<table>
<thead>
<tr>
<th>Industry Scheme</th>
<th>Banking and Financial Services</th>
<th>Government and Public Administration</th>
<th>Manufacturing</th>
<th>Health Care</th>
<th>Education</th>
<th>Retail</th>
<th>Construction</th>
<th>Insurance</th>
<th>Oil and Gas</th>
<th>Technology</th>
<th>Services (Other)</th>
<th>Transportation and Warehousing</th>
<th>Telecommunications and Internet Services</th>
<th>Retail and Other Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases</td>
<td>368</td>
<td>229</td>
<td>192</td>
<td>144</td>
<td>132</td>
<td>104</td>
<td>86</td>
<td>85</td>
<td>74</td>
<td>74</td>
<td>70</td>
<td>60</td>
<td>62</td>
<td>60</td>
</tr>
<tr>
<td>Billing</td>
<td>9.5%</td>
<td>25.3%</td>
<td>32.0%</td>
<td>31.3%</td>
<td>34.1%</td>
<td>15.4%</td>
<td>27.6%</td>
<td>17.6%</td>
<td>20.3%</td>
<td>23.7%</td>
<td>22.9%</td>
<td>22.1%</td>
<td>12.9%</td>
<td>26.7%</td>
</tr>
<tr>
<td>Cash Loss</td>
<td>11.1%</td>
<td>7.9%</td>
<td>5.2%</td>
<td>9.7%</td>
<td>13.6%</td>
<td>12.5%</td>
<td>8.1%</td>
<td>4.7%</td>
<td>4.1%</td>
<td>5.4%</td>
<td>15.7%</td>
<td>4.4%</td>
<td>1.6%</td>
<td>13.3%</td>
</tr>
<tr>
<td>Cash on Hand</td>
<td>17.9%</td>
<td>10.5%</td>
<td>8.3%</td>
<td>11.1%</td>
<td>17.4%</td>
<td>11.5%</td>
<td>7.3%</td>
<td>4.7%</td>
<td>9.5%</td>
<td>8.1%</td>
<td>22.9%</td>
<td>5.9%</td>
<td>4.8%</td>
<td>20.0%</td>
</tr>
<tr>
<td>Check Tampering</td>
<td>9.5%</td>
<td>9.2%</td>
<td>13.5%</td>
<td>14.6%</td>
<td>7.6%</td>
<td>9.6%</td>
<td>10.5%</td>
<td>17.6%</td>
<td>4.1%</td>
<td>5.4%</td>
<td>18.6%</td>
<td>10.3%</td>
<td>6.5%</td>
<td>31.7%</td>
</tr>
<tr>
<td>Corruption</td>
<td>37.5%</td>
<td>38.4%</td>
<td>30.3%</td>
<td>30.0%</td>
<td>31.6%</td>
<td>32.7%</td>
<td>36.0%</td>
<td>28.3%</td>
<td>60.0%</td>
<td>24.5%</td>
<td>26.6%</td>
<td>91.5%</td>
<td>41.9%</td>
<td>16.7%</td>
</tr>
<tr>
<td>Expense Reimbursement</td>
<td>5.4%</td>
<td>15.7%</td>
<td>22.9%</td>
<td>20.1%</td>
<td>15.9%</td>
<td>8.7%</td>
<td>20.9%</td>
<td>9.4%</td>
<td>10.6%</td>
<td>27.0%</td>
<td>12.9%</td>
<td>8.8%</td>
<td>19.4%</td>
<td>16.7%</td>
</tr>
<tr>
<td>Financial Statement Fraud</td>
<td>12.0%</td>
<td>7.9%</td>
<td>10.9%</td>
<td>13.2%</td>
<td>5.3%</td>
<td>5.8%</td>
<td>17.4%</td>
<td>7.1%</td>
<td>6.8%</td>
<td>12.2%</td>
<td>17.1%</td>
<td>5.9%</td>
<td>9.7%</td>
<td>11.7%</td>
</tr>
<tr>
<td>Non-Cash</td>
<td>10.6%</td>
<td>14.8%</td>
<td>30.2%</td>
<td>13.2%</td>
<td>17.4%</td>
<td>32.7%</td>
<td>22.1%</td>
<td>5.9%</td>
<td>17.6%</td>
<td>18.9%</td>
<td>22.9%</td>
<td>20.4%</td>
<td>38.7%</td>
<td>10.0%</td>
</tr>
<tr>
<td>Payroll</td>
<td>8.8%</td>
<td>15.5%</td>
<td>11.5%</td>
<td>9.7%</td>
<td>7.6%</td>
<td>3.8%</td>
<td>16.3%</td>
<td>5.9%</td>
<td>8.1%</td>
<td>2.7%</td>
<td>11.4%</td>
<td>7.4%</td>
<td>3.2%</td>
<td>11.7%</td>
</tr>
<tr>
<td>Register Disbursements</td>
<td>2.7%</td>
<td>1.7%</td>
<td>5.7%</td>
<td>2.1%</td>
<td>1.5%</td>
<td>8.7%</td>
<td>1.2%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>1.4%</td>
<td>5.7%</td>
<td>2.9%</td>
<td>3.2%</td>
<td>1.7%</td>
</tr>
<tr>
<td>Skimming</td>
<td>6.8%</td>
<td>14.0%</td>
<td>8.3%</td>
<td>12.5%</td>
<td>25.0%</td>
<td>17.3%</td>
<td>15.1%</td>
<td>10.6%</td>
<td>8.1%</td>
<td>5.4%</td>
<td>21.4%</td>
<td>11.8%</td>
<td>6.5%</td>
<td>18.3%</td>
</tr>
</tbody>
</table>
CORRUPTION
CORRUPTION

// An employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit

// In most businesses, the most common form of corruption is the payment of kickbacks related to purchases
RED FLAGS FOR CORRUPTION

// Off-book fraud, so very hard to detect
  // Payments often do not go through the organization’s accounting records
  // Payments often paid in cash
// Look for “behavioral” red flags
  // Rapidly increasing purchases from one vendor
  // Excessive purchases of goods and services
  // Too close of a relationship with a vendor
DATA ANALYTICS FOR CORRUPTION

// Compare order quantity to optimal reorder quantity
// Compare purchase volumes/prices from like vendors
// Compare quantities ordered and received
// Check for inferior goods (# of returns by vendor)
// Text analytics (analyze the suspected fraudster’s email....)
BILLING SCHEMES

Fraudster creates false support for a fraudulent purchase, causing the organization to pay for goods or services that are nonexistent, overpriced or unnecessary

- Invoicing via shell company
- Invoicing via an existing vendor
  - False invoicing for non-accomplice vendors
  - Pay-and-return schemes
- Personal purchases with organization’s funds
RED FLAGS/DATA ANALYTICS FOR BILLING SCHEMES

// Vendor attribute analysis

// Trending of vendor activity

// Identification of “high risk” payments

// Text analytics
Vendor addresses match employee addresses
**GEOCODING**

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Vendor Address</th>
<th>Latitude</th>
<th>Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntec</td>
<td>1221 East Kearney Street, Springfield, MO</td>
<td>37.320289</td>
<td>-98.538360</td>
</tr>
<tr>
<td>Devon L. Clark</td>
<td>312 East Warwick Street, Springfield, MO</td>
<td>37.320552</td>
<td>-98.536550</td>
</tr>
</tbody>
</table>

Straight Line Distance = 965 Feet

Vendor authorized by “DLC”
A PICTURE IS WORTH 1,000 WORDS....

AP Manager

Vinny’s Salvage Yard
VENDOR TRENDING ANALYSIS

Vendor: JLM Plumbing  Authorized: Janice L. McPhearson

Test phase

Acceleration as confidence builds

Getting Greedy
TIME SERIES ANALYSIS

**Acceleration Patterns:**
Vendors exhibiting a pattern of increased activity over multiple consecutive periods.

**Valley Patterns:**
Vendors exhibiting a pattern of activity characterized by long periods of inactivity between periods of activity.

**Spike Patterns:**
Vendors exhibiting a pattern of activity characterized by unusually high payments in a single period.

Possible fictitious vendor
Possible abuse of dormant legitimate vendor
Possible abuse of active legitimate vendor
# HIGH RISK VENDOR ATTRIBUTES

<table>
<thead>
<tr>
<th>Vendor ID</th>
<th>Name</th>
<th>Address 1</th>
<th>Address 2</th>
<th>City</th>
<th>State</th>
<th>Zip</th>
<th>Total Payments</th>
<th>Business Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>109</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MS</td>
<td></td>
<td>$70,512.70</td>
<td>UPS STORE</td>
</tr>
<tr>
<td>3126</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MS</td>
<td></td>
<td>6,790.00</td>
<td>UPS STORE</td>
</tr>
<tr>
<td>3145</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MS</td>
<td></td>
<td>1,705.00</td>
<td>UPS STORE</td>
</tr>
<tr>
<td>3189</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TX</td>
<td></td>
<td>600.00</td>
<td>POSTNET</td>
</tr>
</tbody>
</table>
TEXT ANALYTICS FAMILY OF FUNCTIONS

- Network Relationship Mapping
- Emotional Tone Detection
- Digital Forensics
- People Places and Events Extraction
- AI-Based Concept Searching
- Topic Extraction

Evolution of topics, interactions, relationships, and emotions over time
TOPIC EXTRACTION

// Identifies overarching topics prior to reading any email
// Determines whose email is read first
// And, whose is not read at all
The tale of two finance departments from emails between officers and staff....
TONE DETECTION

// Identifies emotional tone of conversations prior to reading any email
// Uses POS tagging
  // Adjectives, adverbs, nouns, verbs
// Priority is tense or nervous tones
// Determines whose email is read first
// Gives us only the emails of interest so we don’t have to read them all
TONE DETECTION POINTS

// Operates under premise that communications have an inherent tone expressed through adjectives, idioms, even emoticons

// Adapted from marketing concept of “sentiment analysis” to flag emails responsive to a certain tone

// Powerful because it doesn’t require any initial starting point or theory
PREDICTIVE CODING

Text Corpus -> Cleansed Data -> Random Sample -> Initial Review -> Historic Sets -> Conceptual Sets

Predictive Coding Tools

Responsive Items
BENEFITS

- Reduction in search time (85 – 95 percent)
- Supplements traditional search
- Reduces human error
EXPENSE REIMBURSEMENTS & PURCHASING CARDS
EXPENSE REIMBURSEMENT/P-CARDS

// Any scheme in which an employee makes a claim for reimbursement or fictitious or inflated business expenses

// Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc.

// Employee purchases personal items and submits and invoice to employer for payment

// Employee purchases goods/services for inappropriate uses and charges to employer for payment
RED FLAGS FOR EXPENSE REIMBURSEMENT/P-CARDS SCHEMES

// Expenses exceed what was budgeted or prior years totals
// Expenses claimed on days employee did not work
// Purchases that do not appear to be business related
// Minimal or non existent support for requests
// Altered receipts
// Unusual or excessive reimbursements to one employee
// Submitted receipts are consecutively numbered
// Expenses in round dollar amounts
// Expenses just below receipt submission threshold
DATA ANALYTICS FOR EXPENSE REIMBURSEMENT/P-CARD SCHEMES

// Identify transactions on weekends, holidays or while employee is on vacation

// Identify split transactions in which a large purchase are split into smaller transactions just under approval threshold

// Identify unusually high or frequent expense reimbursement/p-card usage

// Identify expenses in round dollar amounts
CLOSING THOUGHTS
ONE TOOL IN THE TOOLBOX

// Analytics does not tell the whole story
// It tells you where to start looking
// Creates efficiency in your review process
// Once you understand your data and your environment, you can automate your analytics to repeat on schedule
Agenda

- Introduction
- Emerging Trends in High Tech Fraud
- The Rise of Big Data
- Techniques to Combat High Tech Fraud
- Case Studies
- Implementing a Data Breach Response Program
Objectives of This Presentation

> Raise awareness of the emerging trends in high tech crime, such as how organizations are increasingly vulnerable to high tech fraud

> Establish an understanding of common how Big Data can be leveraged to combat fraud

> Demonstrate how Big Data can be leveraged to detect fraud

> Understand steps that organizations can take to incorporate data mining techniques into their fraud prevention programs
The Rise of Big Data
What is Big Data?

Datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze

- McKinsey Global Institute
Big Data Creates Opportunities for Fraud – Bank of America
Bank of America Manipulated and reordered debits from highest to lowest in order to maximize the number of overdrafts and, consequently, the amount of overdraft fees.
However, through the use of **Data Mining** or **Data Analytics**, Big Data can be harnessed to fight fraud.
What is Data Mining?

Data Mining is “the process of discovering meaningful new relationships, patterns and trends by sifting through data using pattern recognition technologies as well as statistical and mathematical techniques.”

- The Gartner Group
More and more companies are mining their data to create a competitive advantage and garner customer loyalty by tailoring the customer’s experience to the customer.
Target® Uses Data to Identify Pregnant Mothers

- Target assigns every customer a Guest ID number that stores a complete purchase history as well as any demographic information they’ve gathered or bought from third-party providers.
- By analyzing this data, Target is able to deduce which customers were pregnant, and even their due date.
- Target then sends these customers promotions designed to capitalize on the pregnant-mother market.
- There was an instance of an irate father who showed up at a Target location asking why they keep sending his 14-year-old daughter pregnancy promotions.
- He later returned and apologized – his daughter was indeed pregnant.
Similar techniques to those employed by Target can be used to combat fraud.

According to the 2016 ACFE Report to the Nations, 36.7% of surveyed organizations made use of data mining/analysis.

Further, proactive data monitoring was associated with 54% lower losses and fraud detected in ½ the time.
Forensic Data Mining
Forensic data mining uses sophisticated procedures and technologies to identify concealed patterns in financial, non-financial, and textual data that would not otherwise be detectable due to the size and complexity of the data.

- Forensic data mining classifies activities into fraudulent and non-fraudulent behavior.
- The goal is to detect outliers, anomalies, and irregularities.
Why Employ Data Mining Techniques?

> Data mining techniques are efficient and effective
> Data sets are massive in size and often proprietary in format
> “100% analysis is the most effective way to analyze for fraud”
  
  - Dr. Conan Albrecht
  Professor of Information Systems
  Brigham Young University
NYS Inspector General Medicaid Fraud Detection

> NYS Department of Taxation and Finance
> NYS Department of Labor
> NYS Office of Children and Family Services
The aim of Data Mining is to:

> Build a profile of the characteristics of fraudulent behavior
> Pull out the cases that meet the historical characteristics of fraud.
Common Data Mining Target Areas

- Vendors and accounts payable
- Employees and payroll
- Benefit Payments
- Entitlement Programs
- Revenue Collections
- Tax collections
What Data Mining Can Prevent

> Payment error
> Billing and payment fraud
> Inventory fraud
> Check fraud
> Procurement fraud
> Pension scam
The Goal of Data Mining is to Detect Patterns

- Numeric Patterns – fictitious invoice numbers, fictitiously-generated
- Time Patterns – Transactions occurring too regularly, activity at unusual
- Name Patterns – Similar and altered names and addresses
- Geographic Patterns – Proximity relationships between apparently unrelated entities
- Relationship Patterns – Degrees of separation
- Textual Patterns – Detection of “tone” rather than words
Common Forensic Data Mining Techniques
Link Analysis

Linking items that are related but removed by several degrees of separation to mask their relationship

> Find matches for known patterns of interests between linked objects
> Find anomalies by detecting violated known patterns
> Find new patterns of interest (for example, in social networking and marketing and business intelligence)
Latent Semantic Analysis involves concept searching based on tone, recurring themes and communication nuances

- Only 20% of data in an organization is structured data
- 80% is unstructured (not housed in a database)
- Most of today’s commonly used anti-fraud/fraud detection and audit techniques focus on the 20% structured data

- Inside Big Data
The Reach of Forensic Data Analysis

> Forensic Data Mining tools have become increasingly sophisticated
> Practitioners can now analyze the contents of an entire data-set, not just the outliers
> Big Data Analysis tools like CaseWare IDEA® analyze 100% of data rather than just discrepancies
> Practitioners are thus enabled to conduct forensic analysis on large data-sets and zero in on relevant data-points
Benford’s Law

A mathematical theory of leading digits. In 1938, Physicist Frank Bedford theorized that in data sets, the leading digits are distributed in a specific, non-uniform way. This theory is based on a logarithm of probability of occurrence of digits that includes the first digit, second digit, first two digits, last digit, and other combinations of digits.
Benford’s Law enables investigators to predict how often each number 1 through 9 will appear as the first non-zero digit in the data set.

- Can be used to analyze financial data and identify red flags
- If the data doesn't look anything like the distribution predicted by Benford's Law, it may mean the numbers have been manipulated
The Round Numbers Test focuses only on the digits to the right of the decimal point to

- The aim is to detect round numbers
- Indicative of unsupported estimates
Public Sector Data Mining Examples and Advisory
US Health Care Finance Administration needed to isolate the likely causes of payment error by developing a profile of acceptable billing practices and used this information to focus their auditing effort.

- Used audited discharge records, built profiles of appropriate decisions such as diagnosis coding and admission.
- Matched new cases.
- Cases that didn’t match were not audited.
- Detected 50% of past incorrect payments resulting in significant recovery of funding lost to payment errors.

Indiana Center for Database Systems
US Defense Finance & Accounting Service needed to find fraud in millions of Department of Defense transactions and identified suspicious cases to focus investigations:

- Built detection models based on known fraud patterns
- Analyzed all transactions and scored based on similarity to these known patterns
- High scoring transactions were flagged for investigation
- Identified over 1,200 payments for further investigation
- Integrated the detection process

- Indiana Center for Database Systems
Washington State Department of Revenue needed to detect erroneous tax returns and focused audit investigations on cases with the highest likely adjustments

> Utilized previously audited returns
> Modeled adjustment per auditor hour based on return information
> Models scored future returns showing highest potential adjustment
> Maximized auditors’ time by focusing on cases likely to yield the highest return
> Closed the ‘tax gap’

- Indiana Center for Database Systems
Federal employees were committing fraud with their government purchase cards. The program had grown from under $1 billion in 1994 to over $19 billion in 2009

- Took samples to test effectiveness of controls
- Data mined using criteria such as prohibited goods or services or items likely to be for personal use
- Estimated that nearly 41 percent of all federal purchase card transactions from July 1, 2005, through June 30, 2006, failed basic internal control checks
- Found that Federal employees embezzled over $643,000 to pay for gambling, car and mortgage payments, retail purchases, and online dating services
Individuals posed as disaster victims of Hurricanes Katrina and Rita on order to obtain FEMA payments

> Used FEMA’s disaster assistance database to draw a statistical sample for fraud/improper payments
> Identified multiple registrations and duplicate payments
> Compared payments to federal prison databases
> Data mined for inappropriate uses of debit cards
> Revealed over $1 billion in fraud or improper payments, including duplicate payments and payments to ineligible or fictitious individuals

- US Government Accountability Office
Implementing a Data Mining Program
Forensic Data Mining Action Steps

- Obtain a detailed understanding of the process
- Identify key controls and obvious vulnerabilities
- Sample transactions to test the effectiveness of key controls
- Obtain data file of all transactions
Forensic Data Mining Action Steps

> Use data mining and file comparisons to identify unusual transactions
> Analyze supporting documentation
> Consult with investigators and legal counsel to identify improper payments
> Verify that real property was actually recorded in the agency’s property records
Dealing with Fraud in a High-Tech Age

Anne P. Harty, CPA
Chief Financial Officer
City of Rock Hill, SC
Statistics Show...

- Of all industries, government is the second most likely to be impacted by fraud
  1. Corruption
  2. Billing
  3. Non-Cash
  4. Expenses Reimbursement
  5. Check Tampering
  6. Payroll
• We all know basic Internal Controls:
  – Separation of Duties (authorization, recording, reconciling, custody)
  – Surprise Audits
  – Timely Reconciliations
  – Timely Financial Reports
  – Secure Computer Access
  – Central Collections
  – Separate Cash Drawers
  – And more
How can we use technology to prevent and detect fraud?

- By joining various data sets across the organization to find correlations
  - Sorting
  - Filtering
  - Grouping
What are we looking for?

- Irregular activity or patterns
- Prevention of waste
- Duplicate payments of invoices
- Fictitious Vendors
- Matches between employees and vendors
- Improper approval processes
- Circumvention of approval process
- Coercion
- Gaps in numbering
• Paying for items never received
• Paying a legitimate vendor for personal items
• Payroll –
  – Fictitious overtime
  – Fictitious employees
  – Unauthorized raises
  – Terminated employees still being paid or receiving benefits (such as insurance)
What types of data files are we analyzing?

- Vendor lists
- Accounts payable records
- Invoices
- Purchase orders
- Checks and ACH transactions
- Numbers of transactions
- Transactions by amount, by vendor, by week, by month, by year
Computer Assisted Auditing Tools: “CAAT”

- Filtering large amounts of data to efficiently identify irregularities
- Allows for testing of every transaction, rather than a sample
- Allows for real-time continued testing of data to quickly identify irregularities
- Excel data downloads are useful, but special programs are available
Fictitious Vendors

- Compare the mailing addresses of Vendors to the mailing addresses of Employees
- Map mailing addresses on GIS
- Are there different vendors with the same address?
• Matching government data file of checks written to the financial institution records as checks are processed
Invoice Approval

• Have an on-line invoice approval process
• Match approvers to authorization levels
• Verify that the invoice approver matches the authorization for the amount or general ledger department/division
• Did the same employee authorize and approve the invoice?
Receipting/Cash Collections

- Compare transactions by employee
- Compare number of void or credit transactions by employee (cash skimming)
- Match customer name to employee’s names
- Trend void transactions by day of the week, match to employee schedules
• Match employee workers compensation claims to work schedules, liability claims, previous workers compensation claims
• Compare employee spouses/dependents covered on health insurance to beneficiaries in retirement system data
• Match insured employees to payroll files
Purchase Orders

- Match purchase order pricing to invoice pricing
- Match unit pricing to State Contract pricing list
Business Licenses

• Match the local business license file with the retail license file and sales data from the State Department of Revenue

• Request accounts payable files from other Public Entities by FOIA and match to Business License file
Property Taxes

- Map property tax collections in GIS to look for irregularities.
- Up to date aerial photography is useful for finding new building construction or additions not permitted.
- Match building permit files to property tax assessment increases.
- Match property tax amounts against Utility usage records.
• Match property tax map numbers to stormwater charges
• Match property tax file locations and GIS data to Utility billing data
• Match irregular residential electric usage to police crime records
• Require proof of identification to set up new accounts
• Match transaction data to building access data
  – Were transactions performed after normal operating hours? On weekends or holidays?
  – Who enters the building afterhours?
  – Who works late?
• Compare W-2 totals to Human Resources files
• Sort by amount paid – trend over years
• Calculate pay increase percentages for employees over time
• Direct Deposit only - check data for duplicate direct deposit checking account numbers for more than one employee
• Match employee badges, to email addresses, to the employee file
Purchasing Cards

- Match transaction dates to time card data
- Match transaction amounts to authorization levels
The benefit of testing all transactions

• The benefit of testing all transactions prevents excuses such “it was a mistake, repeated over time”, “computer glitch”, “training issue”, “new software”

• Look at entire dataset to help determine when something irregular began

• Most fraud starts small. Small transactions are not excluded
• Sharing of data files can be difficult
• Be careful who you work with - coercion
• Have authority levels and spending levels documented
• Carry fidelity bonds on employees
• Whistleblower Hotline
• Build a culture of honestly and transparency
QUESTIONS?

Shauna Woody-Coussens
swoodycoussens@bkd.com
(816) 701-0250
bkd.com

Anne Harty
anne.harty@cityofrockhill.com

Brian Sanvidge
(212) 792-4836
Brian.Sanvidge@bakertilly.com
bakertilly.com