FACTORS LEADING TO EFFECTIVE INTELLIGENT SOLUTIONS - THE CASE OF FRAUD DETECTION

Duarte Trigueiros,
IMMM 2016, Valencia
FRAUD DETECTION IS USED AS A CASE STUDY TO ILLUSTRATE INTERACTIONS BETWEEN MANAGEMENT PRACTICE, GOVERNANCE RULES AND IT-BASED SOLUTIONS. MISLEADING CLAIMS AND CAUSES OF SUCCESS ARE DISCUSSED.
WHAT IS FRAUD?

Fraud is characterized by:
- Deception or trickery
- Attempt to hide the dishonesty for as long as possible.

Fraud benefit is not restricted to monetary or material benefits and may be
- tangible or
- intangible.
A third party may also obtain a benefit.

“Dishonestly obtaining a benefit by deception or similar means”
CONDITIONS FOR FRAUD TO OCCUR

- **Opportunity** - poorly secured supplies / equipment, access to checkbook, unchecked petty cash register...
- **Motivation** - passed over in promotion, overextended financially, badly needs cash.
- **Justification** - “I’m underpaid anyway, they owe me this.”, “I’m drowning in debit”, “It’s just a small sum. No one will ever notice.”
FRAUD TYPES

- For prevention and detection purposes, frauds are divided in:
  - Internal Fraud: Theft or misuse of assets, false invoicing, entity credit card ...
  - External Fraud: False claim of benefits, tax evasion, identity theft ...
  - Complex: Collaboration between agents to deceive entity or State

- The most common type of internal fraud is known as “occupational” fraud
- Cases of complex fraud involve collaboration between agency employees and external parties.
### Fraud Types

- The three most common types of **internal** fraud:

<table>
<thead>
<tr>
<th>Asset Misappropriation</th>
<th>Corruption</th>
<th>False Financial Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cash</td>
<td>- Accepting bribes</td>
<td>- Earnings manipulation</td>
</tr>
<tr>
<td>- False Invoicing</td>
<td>- Exchanging favors</td>
<td>- Liabilities hiding</td>
</tr>
<tr>
<td>- Payroll</td>
<td>- Nepotism</td>
<td></td>
</tr>
</tbody>
</table>

- Fraud is most likely to occur **in the accounting department**. Accounting staff have the greatest access to resources and have the opportunity and knowledge to hide the fraud.
**Fraud Types**

- The three most common types of *EXTERNAL* fraud:

<table>
<thead>
<tr>
<th>Identity misappropriation</th>
<th>False Claim</th>
<th>Tax Evasion</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Internet</td>
<td>- Insurance</td>
<td>- Income manipulation</td>
</tr>
<tr>
<td>- Card</td>
<td>- Bank Loan</td>
<td>- Benefits</td>
</tr>
<tr>
<td>- Money Laundering</td>
<td>- Suppliers</td>
<td></td>
</tr>
</tbody>
</table>

- Fraud is most likely to occur in the accounting department. Accounting staff generally have the greatest access to resources and have the opportunity and knowledge to hide the fraud.
FRAUD PROFILE

Entities are not similar regarding the risk of fraud:
- Some, are not exposed to external fraud
- Others, are especially exposed to corruption.

In order to prevent fraud, it is important to know:
- the entity’s fraud risk characteristics ("profile")
- within such profile, what are the most likely exposures to consider?
FRAUD PROFILE

- Each entity has its own **risk profile** comprising its **exposures** to different types of fraud.

PROFILE: different types of fraud:
- *Internal*
- *External,*
- *Complex*

Different levels of risk:
- *High*
- *Medium,*
- *Small* … other characteristics of fraud considered in profile
### Fraud Profile

- Each entity has its own fraud risk level:

<table>
<thead>
<tr>
<th>Fraud risk level:</th>
<th>Preventive strategies:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>- Rotation of personnel</td>
</tr>
<tr>
<td></td>
<td>- Security clearances for staff</td>
</tr>
<tr>
<td></td>
<td>- Regular Supplier reviews</td>
</tr>
<tr>
<td></td>
<td>- Independent confirmation of service delivery</td>
</tr>
<tr>
<td></td>
<td>- Supplier and customer screening</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>- Regular and random audit checks</td>
</tr>
<tr>
<td></td>
<td>- Experienced personnel placed in high risk roles</td>
</tr>
<tr>
<td></td>
<td>- Code of conduct</td>
</tr>
<tr>
<td></td>
<td>- Fraud policy</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>- Fraud awareness training</td>
</tr>
<tr>
<td></td>
<td>- Employment screening</td>
</tr>
</tbody>
</table>
**FRAUD CONTROL**

- Is the operational level of a hierarchy where Ethical conduct and sound Governance rules are the upper levels.
- Effective fraud control requires **commitment from the top**, together with a **fraud awareness culture** which is pervasive inside the organization.
- **Prevention, detection** (fraud control operations) are of little use when there is no strategic commitment to fraud control.
**Fraud Control**

- Effective fraud control also requires an overall **governance structure** that reflects the operating environment of an entity.
- When developing or maintaining a fraud control governance structure, an entity needs to ensure it has considered the **three conditions** for fraud to occur:
  - Opportunity
  - Motivation
  - Justification
  
  \[ \text{Opportunity} + \text{Motivation} + \text{Justification} = \text{Increased Fraud likelihood} \]
Governance structure

Comprises, in the case of large entities,
  • Fraud Control Officer,
  • Internal Auditor,
  • Audit Committee
There should be in place:
  • Fraud Control Plan
  • Risk assessment
**FRAUD CONTROL - KEY STEPS**

Four key steps forming the Fraud Control Lifecycle:

- **Fraud prevention**: strategies designed to prevent fraud from occurring in the first instance.
- **Fraud detection**: strategies to discover fraud as soon as possible after it has occurred.
- **Fraud response**: systems and processes that assist an entity to respond appropriately to an alleged fraud.
- **Fraud monitoring**: responsibilities are being met, accountability is promoted, compliance with fraud control strategies is demonstrated.
Fraud Control increases non-productive costs:
- Directly in order to perform the four control phases
- Indirectly by reducing operational performance
- Negative effects on customer satisfaction

**Pareto principle:**
an increase in costs do not lead to the corresponding increase in effectiveness
Resources available for fraud control are in **limited**. **Should** be limited.

Planning fraud control activities must be based on **priority areas** in terms of success in meeting primary objectives.

The following table provides examples of fraud controls that could be used in each phase of a fraud control program.
<table>
<thead>
<tr>
<th>Phase of a fraud control program</th>
<th>Examples of fraud controls to implement</th>
</tr>
</thead>
</table>
| **Policy development, program design and business case** | Fraud risk assessment  
Fraud control plan  
Employment screening  
Communication and awareness |
| **Procurement strategy** | Rigorous, transparent tender processes  
Screening of suppliers and customers  
Segregation of duties on selection and approval of procurements |
| **Delivery / implementation / management** | Regular supplier reviews, also by surprise  
Data mining / analysis  
Reporting mechanisms: hotlines, website, internal reporting channels  
Response to identified / reported frauds  
Management / internal audit review of internal controls |
| **Closure** | Management / internal audit review of program closure and expenditure |
FRAUD PREVENTION - KEY ELEMENTS

- fraud policy and Code of Conduct
- fraud risk management processes
- fraud control plan
- employee and third party screening
- fraud awareness training
- explicit controls for activities with high exposure
- internal publicity of fraud investigation outcomes
# Fraud Prevention - Public Sector Examples of Exposure

<table>
<thead>
<tr>
<th>Entity or function</th>
<th>Examples of fraud exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Civil servant makes improper use of inside information, or uses authority to gain commercial benefit or other advantage.</td>
</tr>
<tr>
<td>Procurement</td>
<td>Official who benefits from procurement decisions involving expenditure of public money. Collusion with suppliers.</td>
</tr>
<tr>
<td>Revenue collection</td>
<td>Tax evasion and fraud associated with social, health, and welfare payments: provision of incorrect information in order to secure payments for which the recipient is not entitled.</td>
</tr>
<tr>
<td>Delivery to the public</td>
<td>Contracting (or outsourcing): service provider who charge the State for goods or services that are not delivered, or delivered in an incomplete way.</td>
</tr>
<tr>
<td>Regulatory authority</td>
<td>Official approves compliance with regulatory requirements in exchange for a benefit or advantage.</td>
</tr>
</tbody>
</table>
FRAUD DETECTION
- TYPES

Detection requires properly designed fraud control - or a tip from an employee. Accidental detection of fraud is very unlikely.

- Two types:
**Fraud Detection - Types**

- **Passive measures**
  - Internal Controls
  - Mechanisms to report
  - Tip-Off Hotline
  - Whistle-blowing

- **Active measures**
  - Red Flags Analysis
  - Financial Statement
  - Hot-Spot Analysis
  - Data Mining

**Do not require involvement of management.**

**Require involvement of management.**
Fraud Detection - Internal Controls

- regular independent reconciliation of accounts;
- independent confirmation of service delivery where suppliers are paid in advance for services
- physical security, for example, security cameras
- staff who know their jobs are more likely to identify anomalies
- job rotation / mandatory leave
- comparisons between budgeted and actual figures and the follow-up of discrepancies
- audit trails
- exception reporting
- quality assurance
- surprise audits
- management review
FRAUD DETECTION
- TIP-OFF OR HOTLINE FACILITIES

A single point of contact to report on suspected fraud, independent from management.

- provides access to a trained interviewer,
- operates 24 hours a day,
- supports a multilingual capability,
- provides a phone number that is toll-free,
- applies consistent protocols for gathering and recording relevant information,
- matters reported are normally treated confidentially.
# Fraud Detection - Red Flags

<table>
<thead>
<tr>
<th>Early warnings: people</th>
<th>Early warnings: areas or activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwillingness to share duties/take leave</td>
<td>Financial information inconsistent with performance indicators</td>
</tr>
<tr>
<td>Refusal to implement internal controls</td>
<td>Abnormally high costs in a specific cost center function</td>
</tr>
<tr>
<td>Close association with vendor or customer</td>
<td>Dubious record keeping</td>
</tr>
<tr>
<td>Lifestyle above apparent financial means</td>
<td>High overheads</td>
</tr>
<tr>
<td>Failure to keep records and provide receipts</td>
<td>Bank reconciliations not up to date</td>
</tr>
<tr>
<td>Chronic shortage of cash</td>
<td>Inadequate segregation of duties</td>
</tr>
<tr>
<td>Past legal problems including minor thefts</td>
<td>Reconciliations not performed regularly</td>
</tr>
<tr>
<td>Addiction problems</td>
<td>Small cash discrepancies</td>
</tr>
</tbody>
</table>
Mapping dangerous spots: allegations raised through hotlines and other methods can be analyzed to show hot spots of potential fraud.

The fraud risk exposure profile of an entity should identify positions of officials who, because of the nature of that position, may be vulnerable to fraud. For these:

- regular performance appraisals, mandatory disclosure of interests, assets, hospitality and gifts
- close monitoring in relation to existing computer data-mining to detect transactions that depart from norms
FRAUD DETECTION - DATA-MINING

Analysis of large volumes of transactions using IT and Statistical tools - rather than relying on sampling

- Analysis of suspicious transactions
duplicate payments or claims

- Identification of unusual relationships
  employee bank account matches a vendor bank account

- Assessing the effectiveness of internal controls
  password sharing, employees on the payroll after termination

- Identification of irregular trends over periods of time
  supplier favoritism

- …
Once detected, fraud must be investigated and action taken.

**Response - Investigation**

- Investigated
- Action taken
- Response to fraud

**Prevention**

- Detection
- Response
- Monitoring
RESPONSE
- ACTION

Action

Criminal prosecution
- Is evidence sufficient?
  - Decision not to prosecute - at highest level

Civil or administrative remedies
- Policy must be pre-defined
  - Transfer, suspension, expulsion,…

Recovery procedure
- Agreement
  - Civil procedure
    - Through Court
MONITORING
- KNOWLEDGE EXTRACTION

Monitoring of fraud control assist managers to:
- assess the relevance of fraud strategies
- test whether fraud strategies target desired population
- find more effective ways of combating fraud

Evaluations also establish **causal links** such as:
- balance between fraud prevention and detection strategies
- weighting of entity incentives to reduce potential losses from fraud as opposed to discovering fraud after it has occurred

Analysis can also be made on the effectiveness of established controls through cost / benefit analysis both pre- and post-implementation of fraud controls.
MONITORING
- REVIEW OF FRAUD CONTROL PLAN:

- ensure risk assessments have been made
- awareness-raising and training are evaluated and are shown to work well in practice
- allegations recorded, analyzed and followed-up
- cases of fraud are dealt with according to applicable external and internal standards
- remedies are applied appropriately
- information on cases of fraud are used to update the fraud risk profile and strengthen controls
- accurate information is provided to the Audit Committee on a timely basis
IS FOR FRAUD DETECTION
- TYPES

- **Internal fraud**: in well-known business processes
  - General purpose boxes of tools for file analyses
  - Automation is never achieved; detection is periodically performed

- **External fraud**: industries with high-risk processes
  - Dedicated, embedded models, real-time analysis of each transaction
Two well-known players (low- and high-end) are

- “IDEA”, “CaseWare” (and other products) from “Audimation” http://www.audimation.com/ is aimed at small- medium-sized entities, not expensive, offering little field support or training.

- ACL Analytics (and other) from ACL http://www.acl.com middle-large-sized entities, offering the full-range of services including the deployment of specialists into customers’ sites.

There is a multitude of other players: 45 vendors are listed at http://www.capterra.com/financial-fraud-detection-software/
IS FOR FRAUD DETECTION
- INTERNAL – TYPICAL TASKS 1

- Look for duplicate payments made fraudulently by an employee in collusion with a vendor.
- Look for duplicate purchases made using payment- or credit-cards within a short time. One of the purchases may be for personal use.
- Compare recent and previous versions of master files of the entity’s ERP database to see if the file has been changed in a fraudulent way.
- Examine control settings of the same key files, searching for fraudulent changes: a manager may modify the permitted maximum purchase amount from 5,000 to 50,000 just during a few minutes.
IS FOR FRAUD DETECTION
- INTERNAL – TYPICAL TASKS 2

- Non-authorized expenses: examine dates (weekend purchases are suspect), vendor code or purchase description. Split transactions are also suspect.

- Compare suppliers’ and payments’ data with human resources records to search for “phantom vendors” set by employees to their advantage. Some type of loose matching is required in order to overcome variations in the spelling and position of words.

- Compute monthly total purchases by employee (fuel cards, meals’ cards, air-tickets and hotel expenses, purchase- and credit-card use and others). Higher than average purchases may indicate fraud.
IS FOR FRAUD DETECTION
- INTERNAL - TOOLS 1

Use logarithmic-transformed money amounts and other accumulations

Calculated field: Logarithmic axis for money amounts
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benford’s Law</strong></td>
<td>The frequency distribution of first and second digits in a large set of amounts exhibit known pattern. If the observed frequency distribution doesn’t follow such pattern there may be a cause for review.</td>
</tr>
<tr>
<td><strong>Duplicates</strong></td>
<td>Identifies duplicate items within a specified field in a file: identify duplicate billings of invoices and others.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Creates a file in different software format: Excel, Word. Export customer address information to Word for “Mail Merging to customer confirmation letters.”</td>
</tr>
</tbody>
</table>
IS FOR FRAUD DETECTION
- INTERNAL - TOOLS 2

Benford’s Law
**IS FOR FRAUD DETECTION**  
**- INTERNAL - TOOLS 3**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extract / Filter</strong></td>
<td>Extracts specified items from one file and copies them to another file, normally using “if” statement.</td>
</tr>
<tr>
<td><strong>Gaps</strong></td>
<td>Identifies gaps within a specified field in a file: identify any gaps in check sequence or others.</td>
</tr>
<tr>
<td><strong>Index / Sort</strong></td>
<td>Sorts a file in ascending or descending order: sorting a file by social security number to see if any blank or “99999” numbers exist.</td>
</tr>
<tr>
<td><strong>Join / Relate</strong></td>
<td>Combines specified fields from two different files into a single file using key fields, creating relational databases on key fields. It can also be done in an unmatched fashion to identify differences between data files.</td>
</tr>
</tbody>
</table>
## IS for Fraud Detection - Internal - Tools 4

<table>
<thead>
<tr>
<th>Tools</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>Calculates a variable balance such as net sales based on other related variables: product purchases, inventory, etc.</td>
</tr>
<tr>
<td>Sample</td>
<td>Creates random or monetary unit samples from a specified population.</td>
</tr>
<tr>
<td>Statistics</td>
<td>Calculates statistics on a selected numeric field: total positive items, negative items, average balance, etc.</td>
</tr>
<tr>
<td>Stratify</td>
<td>Counts the number, total dollar value, largest, smallest, and average of records of a population falling within specified intervals.</td>
</tr>
<tr>
<td>Aggregate</td>
<td>Accumulates numerical values based on a specified key field: travel and entertainment expense amounts by employee to identify unusually high payment amounts.</td>
</tr>
</tbody>
</table>
IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 1

180,000 payments made by a company
180,000 payments made by a company
IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2
IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2

Matrix of $O$-Anomaly by Repeat

<table>
<thead>
<tr>
<th>$O$-Anomaly</th>
<th>1</th>
<th>10</th>
<th>11</th>
<th>13</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>177240</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2757</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>T</td>
<td>4348</td>
<td>80</td>
<td>11</td>
<td>117</td>
<td>4041</td>
<td>444</td>
<td>196</td>
<td>100</td>
<td>30</td>
<td>56</td>
<td>15</td>
<td>54</td>
</tr>
</tbody>
</table>

Cells contain: cross-tabulation of fields (including missing values)
IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2
IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2

Benford’s
IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2
IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2
IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2
# IS FOR FRAUD DETECTION

## INTERNAL – EXAMPLE 2

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Day</th>
<th>Date</th>
<th>Vendor Number</th>
<th>Inv Number</th>
<th>Amount</th>
<th>Log Amount</th>
<th>First_Two_Digits</th>
<th>Repeat</th>
<th>$O-Anc</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>10</td>
<td>19</td>
<td>2007-10-19</td>
<td>5865 6341357404-1</td>
<td></td>
<td>50.250</td>
<td>1.701</td>
<td>50</td>
<td>9</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>9</td>
<td>7</td>
<td>2007-09-07</td>
<td>5865 000000E2461-1</td>
<td></td>
<td>50.650</td>
<td>1.706</td>
<td>50</td>
<td>7</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>4</td>
<td>11</td>
<td>2008-04-11</td>
<td>4325 W12EK0586...</td>
<td></td>
<td>50.210</td>
<td>1.701</td>
<td>50</td>
<td>7</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
<td>13</td>
<td>2008-03-13</td>
<td>14728 SEE ATT. BAL</td>
<td>500000.0...</td>
<td>5.099</td>
<td>50</td>
<td>4</td>
<td></td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
<td>11</td>
<td>2008-03-11</td>
<td>16487 1750262-02-2</td>
<td></td>
<td>502.580</td>
<td>2.701</td>
<td>50</td>
<td>4</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>5</td>
<td>1</td>
<td>2008-05-01</td>
<td>5063 056832751/00</td>
<td></td>
<td>50.830</td>
<td>1.704</td>
<td>50</td>
<td>4</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>5</td>
<td>1</td>
<td>2008-05-01</td>
<td>5063 056832751/00</td>
<td></td>
<td>50.830</td>
<td>1.704</td>
<td>50</td>
<td>4</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>11</td>
<td>22</td>
<td>2007-11-22</td>
<td>2817 99-5</td>
<td></td>
<td>500971.5...</td>
<td>5.706</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>11</td>
<td>22</td>
<td>2007-11-22</td>
<td>2817 99-5</td>
<td></td>
<td>501057.000</td>
<td>4.700</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>7</td>
<td>29</td>
<td>2007-07-29</td>
<td>5832 240134732703</td>
<td></td>
<td>50.480</td>
<td>1.703</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>6</td>
<td>7</td>
<td>2008-07-07</td>
<td>10242 513284</td>
<td></td>
<td>50.000</td>
<td>1.699</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>6</td>
<td>7</td>
<td>2008-07-07</td>
<td>10242 513284</td>
<td></td>
<td>50.000</td>
<td>1.699</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>6</td>
<td>7</td>
<td>2007-07-07</td>
<td>10242 513284</td>
<td></td>
<td>50.000</td>
<td>1.699</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>7</td>
<td>7</td>
<td>2008-07-07</td>
<td>10242 513284</td>
<td></td>
<td>50.000</td>
<td>1.699</td>
<td>50</td>
<td>3</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>9</td>
<td>4</td>
<td>2007-09-04</td>
<td>17284 310000</td>
<td></td>
<td>502132.1...</td>
<td>5.701</td>
<td>50</td>
<td>2</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
<td>11</td>
<td>2008-03-11</td>
<td>14728 SEE BAL REPT</td>
<td></td>
<td>500000.0...</td>
<td>5.690</td>
<td>50</td>
<td>2</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
<td>10</td>
<td>2008-03-10</td>
<td>16721 SEE ATT. BAL</td>
<td></td>
<td>500000.0...</td>
<td>5.690</td>
<td>50</td>
<td>2</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>2</td>
<td>19</td>
<td>2008-02-19</td>
<td>16721 SEE ATTACH..</td>
<td></td>
<td>500000.0...</td>
<td>5.690</td>
<td>50</td>
<td>2</td>
<td>T</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
<td>25</td>
<td>2008-03-25</td>
<td>16721 SEE ATTACH B</td>
<td></td>
<td>500000.0...</td>
<td>5.690</td>
<td>50</td>
<td>2</td>
<td>T</td>
</tr>
<tr>
<td>2007</td>
<td>8</td>
<td>20</td>
<td>2007-08-26</td>
<td>6099 30110</td>
<td></td>
<td>5084.040</td>
<td>3.700</td>
<td>50</td>
<td>2</td>
<td>F</td>
</tr>
</tbody>
</table>
IS FOR FRAUD DETECTION
- INTERNAL: DIFFICULTIES

- requires knowledge of where to look for fraud
- staff must be familiar both with entity’s data and IS
- many exceptions and false positives
- internal IS tasks are not amenable to automation
  - changes lead to the need to rebuild detecting processes
  - exceptions and false positives must be recognized
  - common-sense must be exercised every minute
- steep learning curve, based on experience
- importing data often difficult or impossible
IS FOR FRAUD DETECTION
- EXTERNAL – TYPICAL TASKS

- Insurance and Government – fraudulent claims,
- Bank loan application – false statement
- Healthcare false billings,
- Retail post-of-sale or Internet and others
  ... identity theft underlies several such frauds

EXAMPLE: fraud in claims of farm subsidies:

<table>
<thead>
<tr>
<th>id</th>
<th>region</th>
<th>farm size</th>
<th>rain fall</th>
<th>land quality</th>
<th>farm income</th>
<th>main crop</th>
<th>claim type</th>
<th>claim value</th>
</tr>
</thead>
<tbody>
<tr>
<td>id601</td>
<td>midlands</td>
<td>1480</td>
<td>30</td>
<td>8</td>
<td>330729 wheat</td>
<td>wheat</td>
<td>decommission_land</td>
<td>74703,1</td>
</tr>
<tr>
<td>id602</td>
<td>north</td>
<td>1780</td>
<td>42</td>
<td>9</td>
<td>734118 maize</td>
<td>maize</td>
<td>arable_dev</td>
<td>245354</td>
</tr>
<tr>
<td>id605</td>
<td>north</td>
<td>1700</td>
<td>46</td>
<td>8</td>
<td>621148 wheat</td>
<td>wheat</td>
<td>decommission_land</td>
<td>122006</td>
</tr>
<tr>
<td>id606</td>
<td>southeast</td>
<td>1580</td>
<td>42</td>
<td>7</td>
<td>445785 maize</td>
<td>maize</td>
<td>arable_dev</td>
<td>122135</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>... total of 298 claims</td>
</tr>
</tbody>
</table>
IS FOR FRAUD DETECTION
- EXTERNAL - EXAMPLE

Diff

Compute diff as a %

Use arable dev only

Type

Predict Claim Value

Farm grant data

discard two cases

Compute official Inc. vs $N-claim_value vs ch

Claim Value pred

Income distribution

Estimated vs real inc

Dist of Difference

Compute difference

Claim vs predicted ch

Identify fraud case

Difference > 50,000
IS FOR FRAUD DETECTION
- EXTERNAL - EXAMPLE

1. Diff
2. Compute IT as a %
3. Use arable dev only
4. Type
5. Predict Claim Value

- Farm grant data
- Discard two cases
- Compute official Inc.
- $N - claim_value vs. cl.
- Claim Value pred

- Income distribution
- Estimated vs real inc.
- Dist. of Difference
- Compute difference
- Claim vs predicted cl.

- Identify fraud case
- Difference > 50,000
IS FOR FRAUD DETECTION
- EXTERNAL - EXAMPLE

- Farm grant data
- discard two cases
- Compute official Inc.:
- $\text{N-claim}_\text{value} \times \text{cl}.
- Claim Value predicted
- Income distribution
- Estimated vs real inc.
- Dist. of Difference
- Compute difference
- Claim vs predicted cl.

- Identify fraud case
- Difference > 50,000

- Compute $\text{IT as a %}$
- Use arable dev only
- Type
- Predict Claim Value
IS FOR FRAUD DETECTION
- EXTERNAL - TASK

Detection is carried out in real time, embedding in the transaction processing software, one or several complex models able to check the plausibility of transactions:
IS FOR FRAUD DETECTION
- EXTERNAL - TASK

Complex models
1. **learn** fraud patterns from previous, detected cases
2. **recognize** transactions where such pattern is present
IS FOR FRAUD DETECTION
- EXTERNAL - DIFFICULTIES

- Complex models require good-quality, documented data on fraud and non-fraud to learn the underlying pattern. Each type of fraud requires its own dataset. In some cases such data does not exist or is small.
- Some fraud areas are not yet contemplated by extant research or they are too broad (identity theft)
- In other areas results are bad:
  - Credit card fraud is the object of much research and results are good; but
  - results are not convincing in Financial Statement fraud detection, also a much researched area.
- **False positives** are a constant burden; and, in some cases, they may exasperate customers.
IS FOR FRAUD DETECTION
- EXTERNAL - VENDORS

- ACL may detect external fraud through continuous transaction analysis in, for example, SAP software [http://www.acl.com/solutions/products/acl-direct-link/](http://www.acl.com/solutions/products/acl-direct-link/)
- SAP has native fraud detection models embedded in transaction-processing products [http://www.sap.com](http://www.sap.com)

