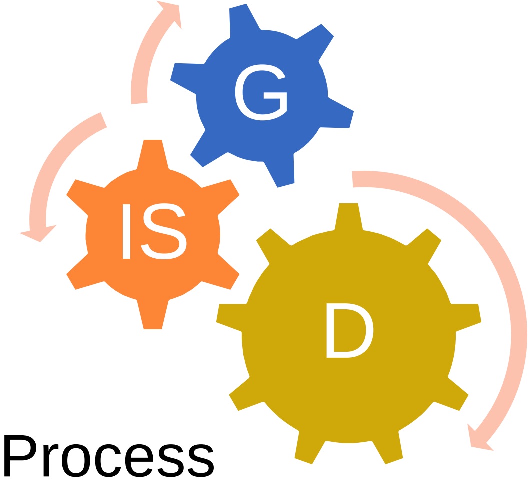
FACTORS LEADING TO EFFECTIVE INTELLIGENT SOLUTIONS - THE CASE OF FRAUD DETECTION

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.



Fraud Detection Process

What is Fraud?

“Dishonestly obtaining a benefit by deception or similar means”

Fraud is characterized by:

- Deception or trickery
- Attempt to hide the dishonesty for as long as possible.

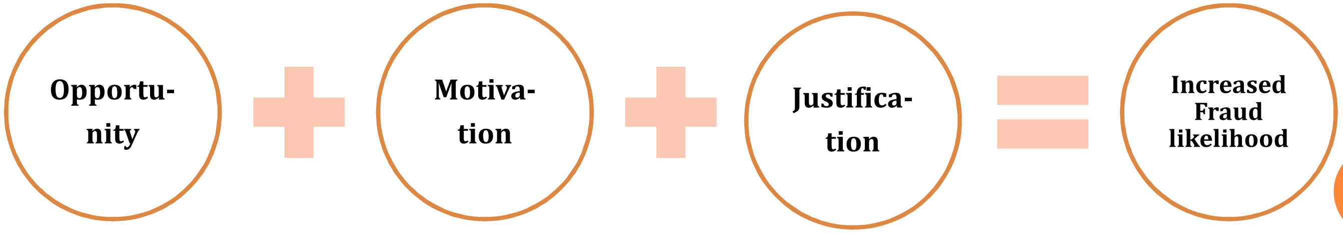
Fraud benefit is not restricted to monetary or material benefits and may be

- tangible or
- intangible.

A third party may also obtain a benefit.

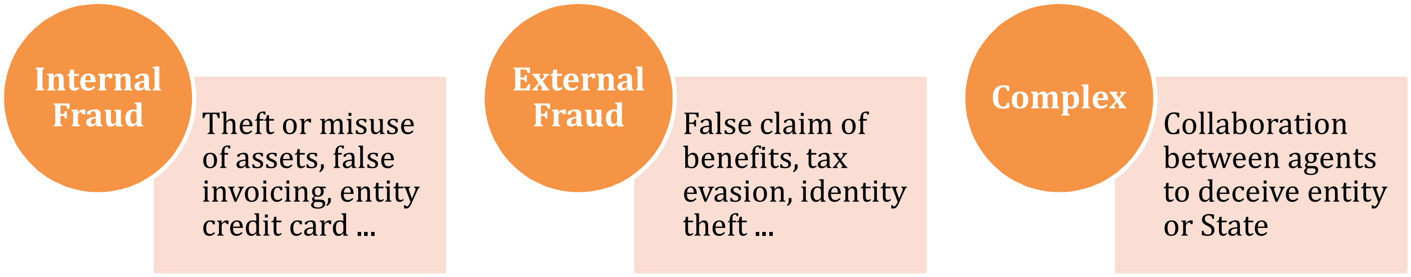
CONDITIONS FOR FRAUD TO OCCUR

- **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 ...

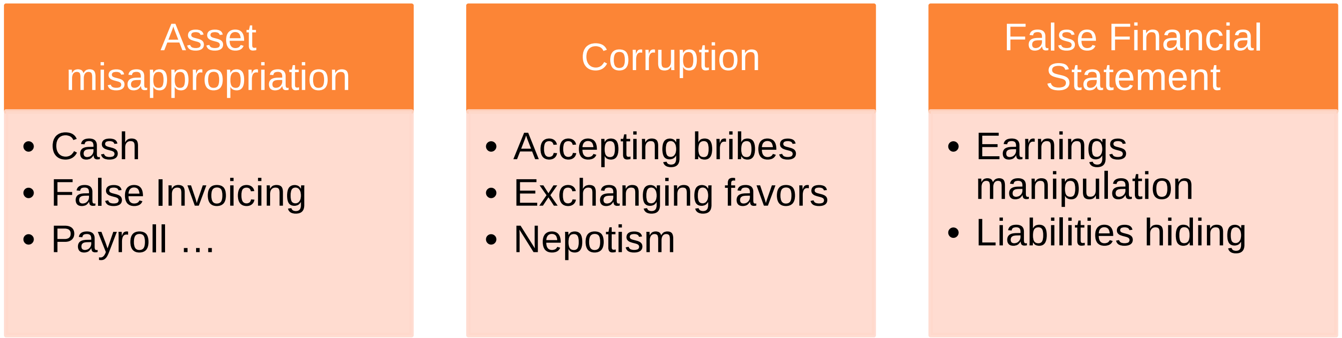
Complex

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:



Asset misappropriation

- Cash
- False Invoicing
- Payroll …

Corruption

- Accepting bribes
- Exchanging favors
- Nepotism

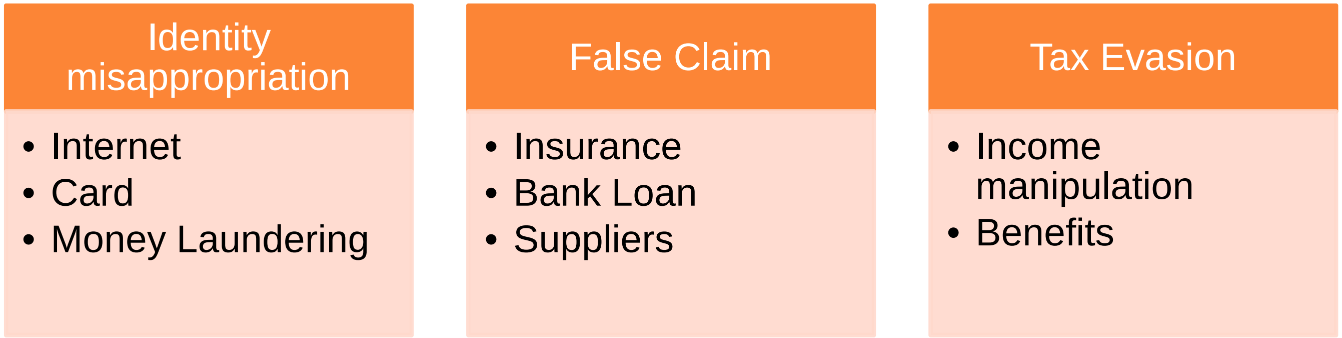
False Financial Statement

- Earnings manipulation
- Liabilities hiding

- 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:



Identity misappropriation

- Internet
- Card
- Money Laundering

False Claim

- Insurance
- Bank Loan
- Suppliers

Tax Evasion

- Income manipulation
- Benefits

- 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:

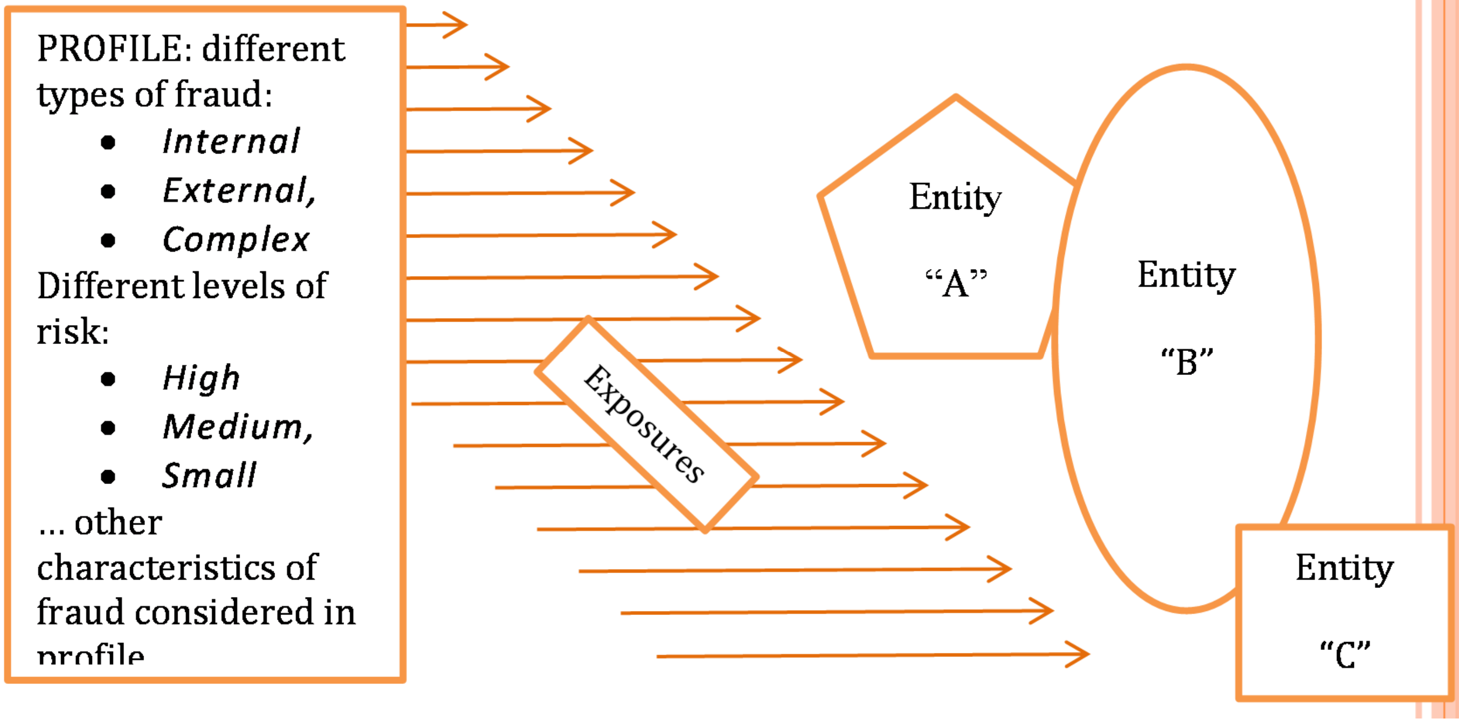
- Some, are not exposed to external fraud
- Others, are especially exposed to corruption.

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*

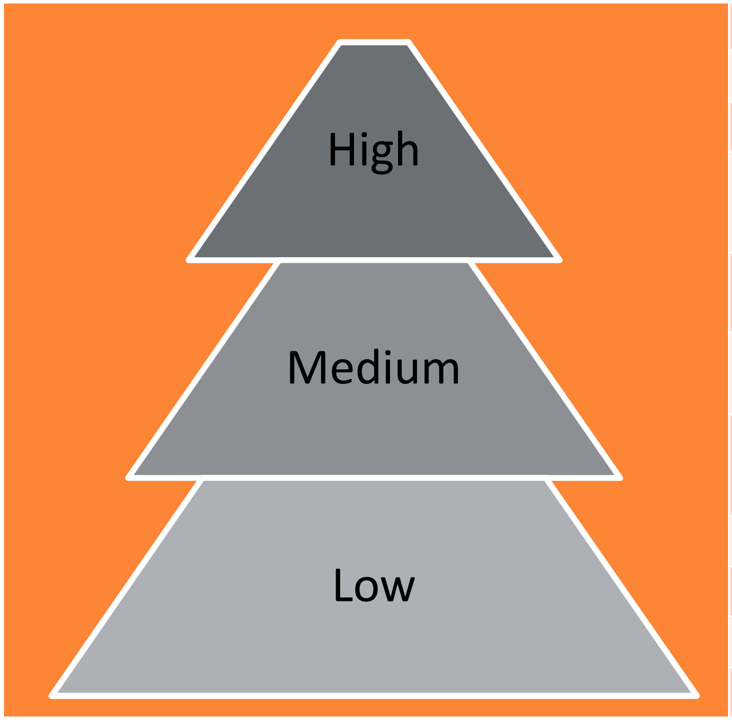
Different levels of risk:

- *High*
- *Medium,*
- *Small*

... other characteristics of fraud considered in profile

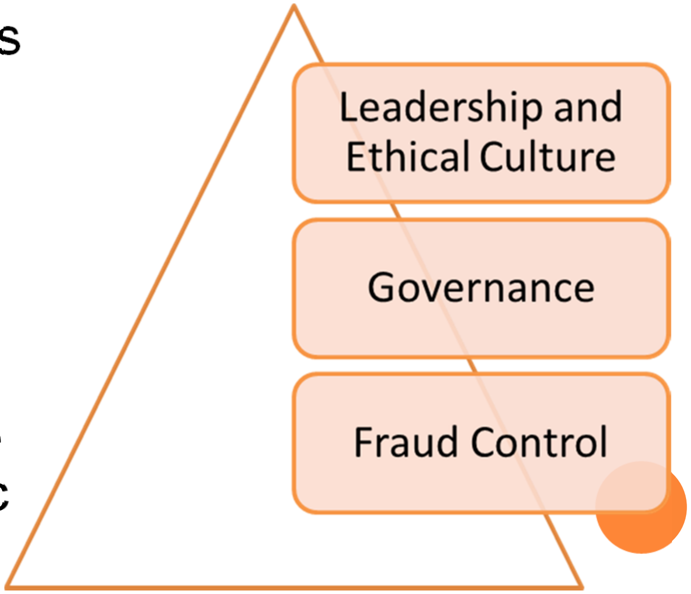
FRAUD PROFILE

- Each entity has its own fraud risk level:

Fraud risk level:	Preventive strategies:
	- Rotation of personnel
	- Security clearances for staff
	- Regular Supplier reviews
	- Independent confirmation of service delivery
	- Supplier and customer screening
	- Regular and random audit checks
	- Experienced personnel placed in high risk roles
	- Code of conduct
	- Fraud policy
	- Fraud awareness training
	- Employment screening

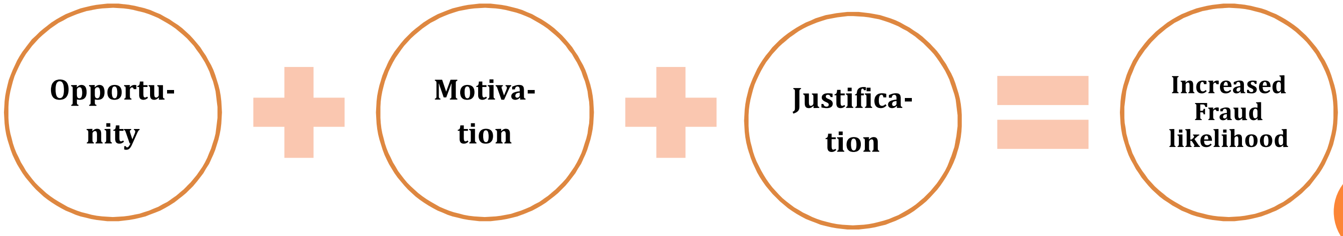
FRAUD CONTROL

- 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 = Increased Fraud likelihood

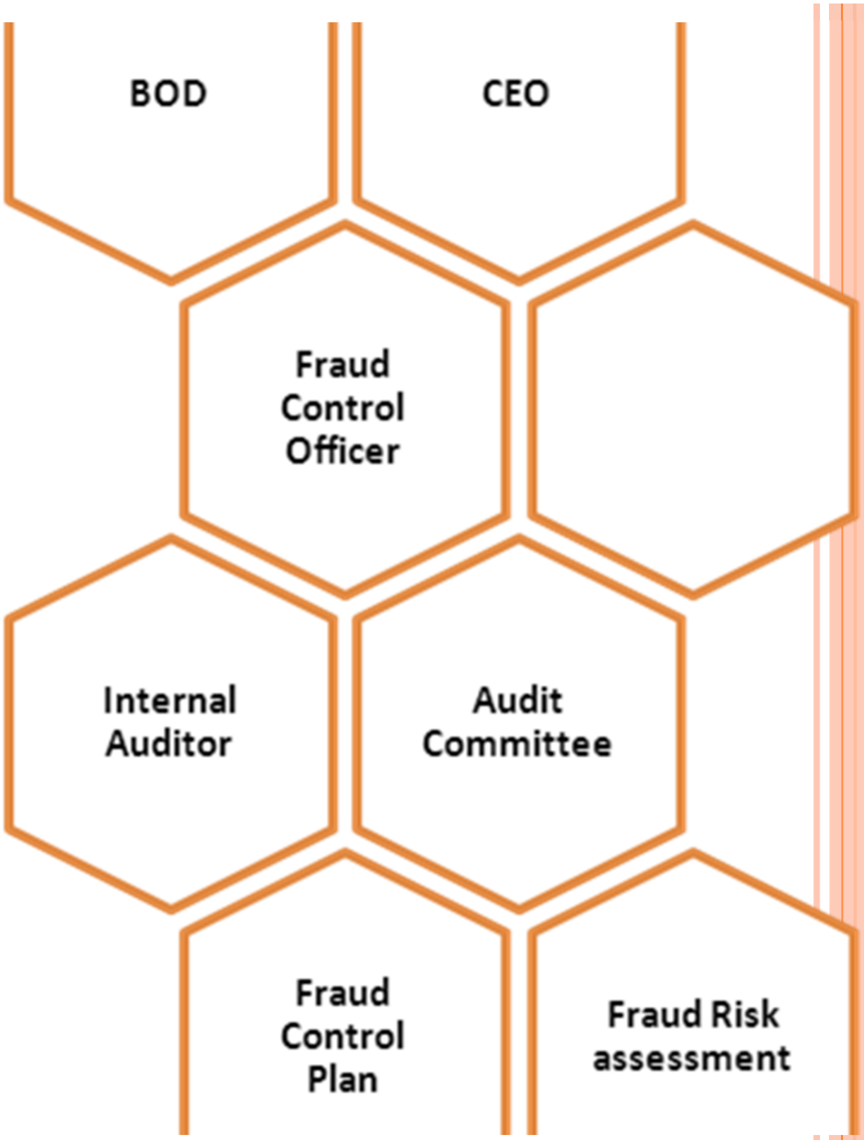
Governance structure

Comprises, in the case of large entities,

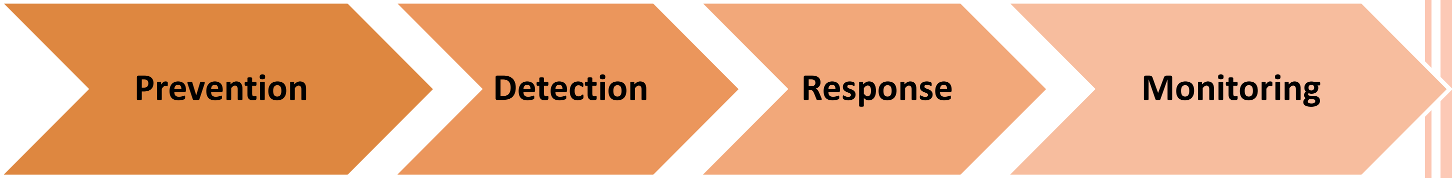
- Fraud Control Officer,
- Internal Auditor,
- Audit Committee

There should be in place:

- Fraud Control Plan
- Risk assessment



Fraud Control - Key steps



Prevention

Detection

Response

Monitoring

Four key steps forming the Fraud Control Lifecycle:

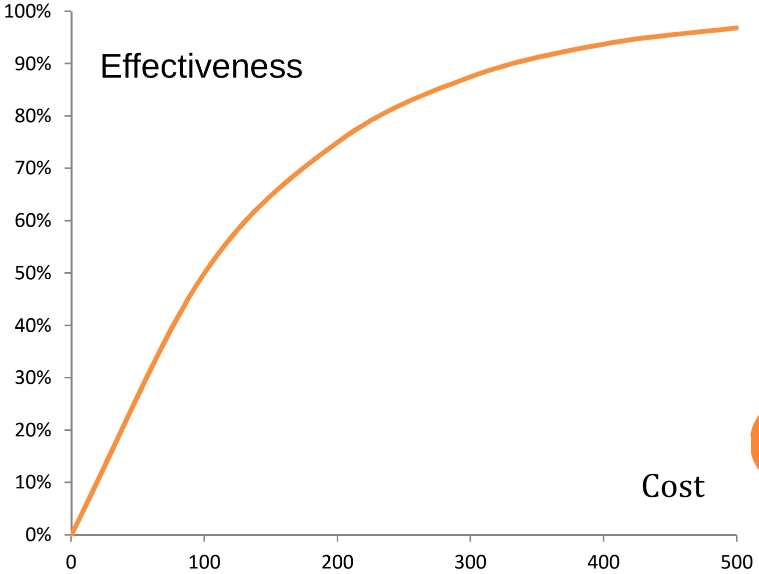
- Fraud prevention: strategies designed to prevent fraud from occurring in the first instance
- Fraud detection: strategies to discover fraud as soon as possible after it has occurred
- Fraud response: systems and processes that assist an entity to respond appropriately to an alleged fraud
- Fraud monitoring: responsibilities are being met, accountability is promoted, compliance with fraud control strategies is demonstrated

Fraud Control - Cost

Fraud Control increases non-productive costs:

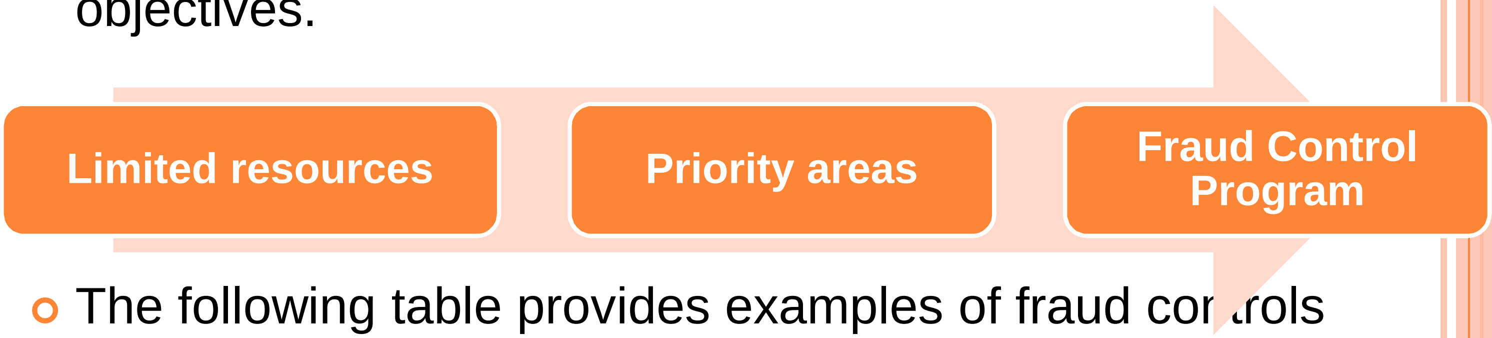
- Directly in order to perform the four control phases
- Indirectly by reducing operational performance
- Negative effects on custom satisfaction

Pareto principle: an increase in costs do not lead to the corresponding increase in effectiveness



Fraud Control
- Cost

- 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.



Limited resources

Priority areas

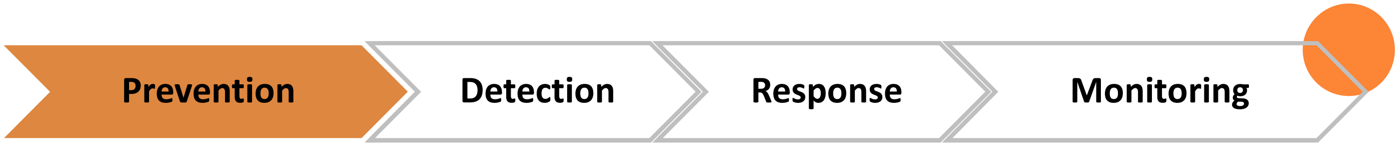
Fraud Control Program

- The following table provides examples of fraud controls that could be used in each phase of a fraud control program.

Phase of a fraud control program	Examples of fraud controls to implement
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

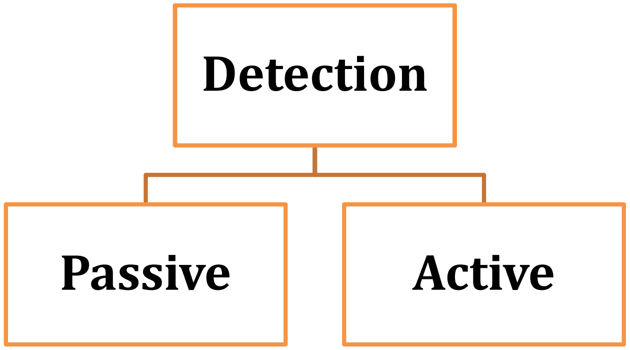
Entity or function	Examples of fraud exposure
Policy	Civil servant makes improper use of inside information, or uses authority to gain commercial benefit or other advantage.
Procurement	Official who benefits from procurement decisions involving expenditure of public money. Collusion with suppliers.
Revenue collection	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.
Delivery to the public	Contracting (or outsourcing): service provider who charge the State for goods or services that are not delivered, or delivered in an incomplete way.
Regulatory authority	Official approves compliance with regulatory requirements in exchange for a benefit or advantage.

Fraud Detection

- Types

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

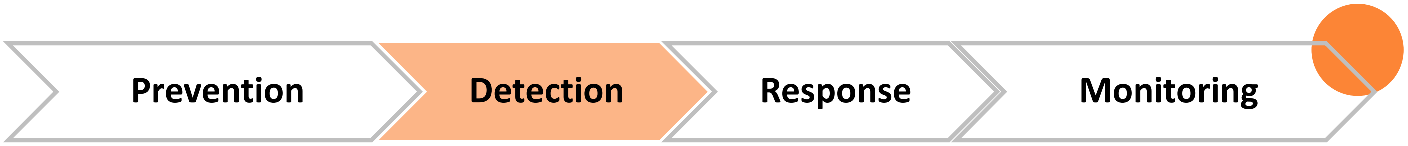
- Two types:



Detection

Passive

Active



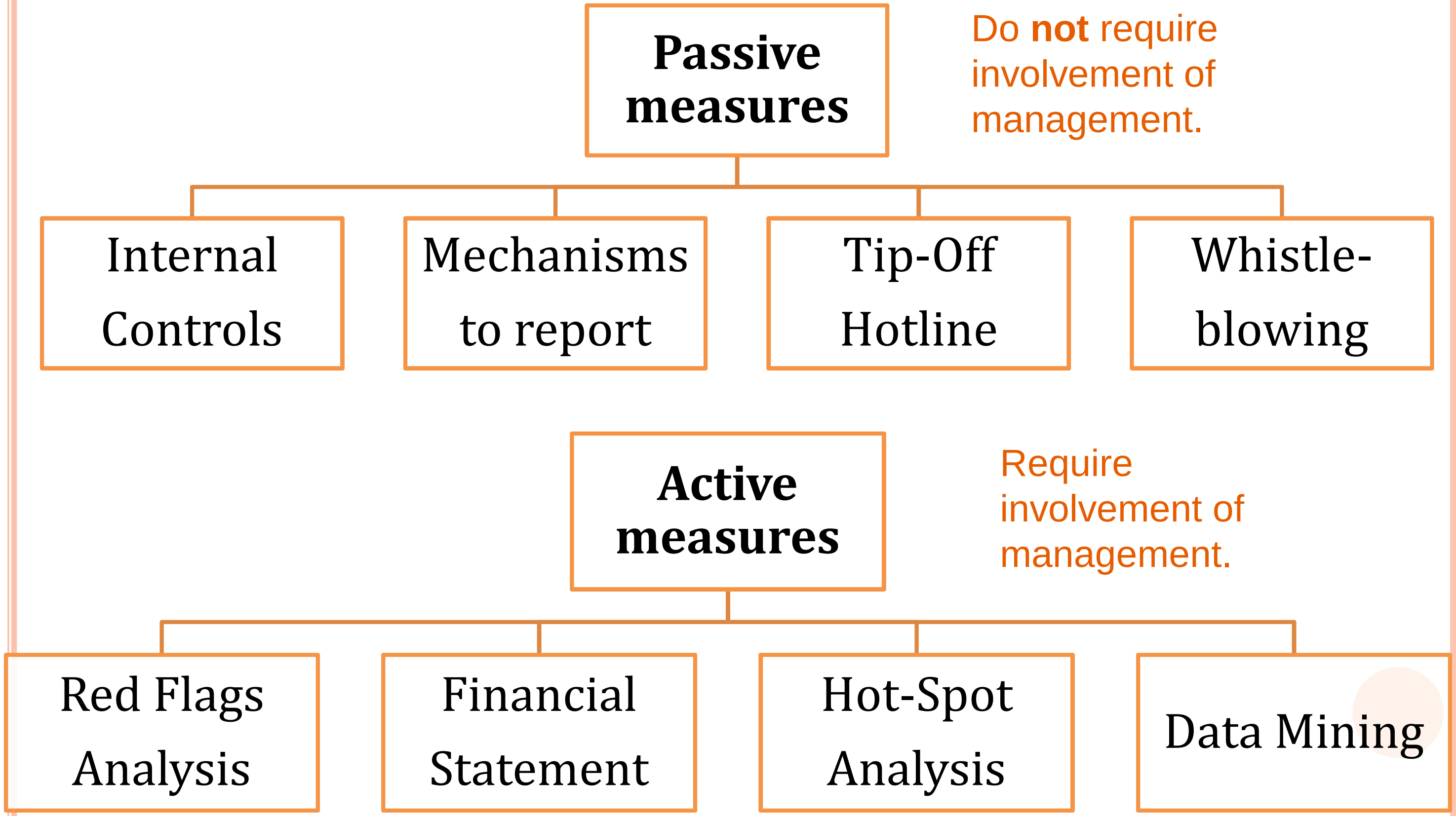
Prevention

Detection

Response

Monitoring

Fraud Detection
- Types



Passive measures

Do **not** require involvement of management.

Internal Controls

Mechanisms to report

Tip-Off Hotline

Whistle-blowing

Active measures

Require involvement of management.

Red Flags Analysis

Financial Statement

Hot-Spot Analysis

Data Mining

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

Early warnings: people	Early warnings: areas or activities
Unwillingness to share duties/take leave	Financial information inconsistent with performance indicators
Refusal to implement internal controls	Abnormally high costs in a specific cost center function
Close association with vendor or customer	Dubious record keeping
Lifestyle above apparent financial means	High overheads
Failure to keep records and provide receipts	Bank reconciliations not up to date
Chronic shortage of cash	Inadequate segregation of duties
Past legal problems including minor thefts	Reconciliations not performed regularly
Addiction problems	Small cash discrepancies

Fraud Detection
- Hot spot analysis

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

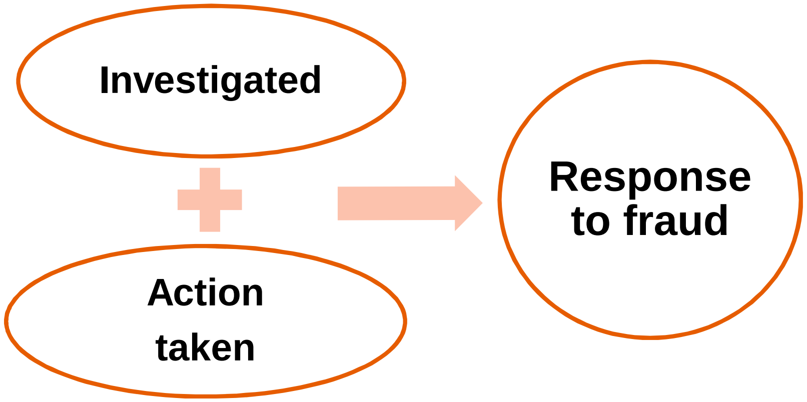
FRAUD DETECTION
- DATA-MINING

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
- …

RESPONSE
- INVESTIGATION

Once detected, fraud must be



Investigated

Action taken

Response to fraud

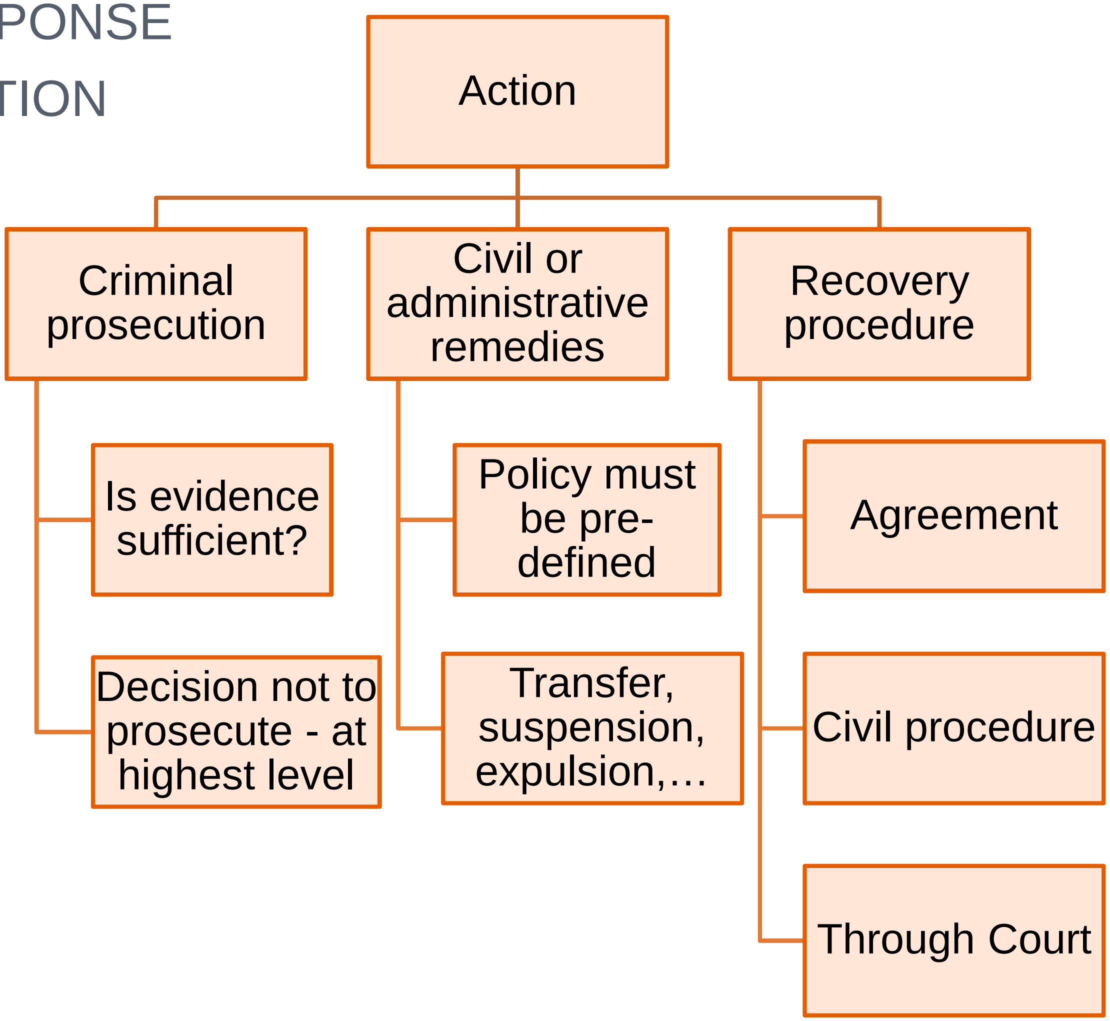
Prevention

Detection

Response

Monitoring

RESPONSE - ACTION



Action

Criminal prosecution

Civil or administrative remedies

Recovery procedure

Is evidence sufficient?

Decision not to prosecute - at highest level

Policy must be pre-defined

Transfer, suspension, expulsion,…

Agreement

Civil procedure

Through Court

MONITORING
- KNOWLEDGE EXTRACTION

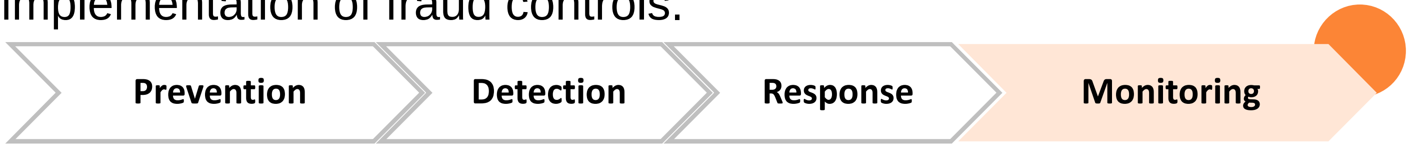
Monitoring of fraud control assist managers to:

- 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

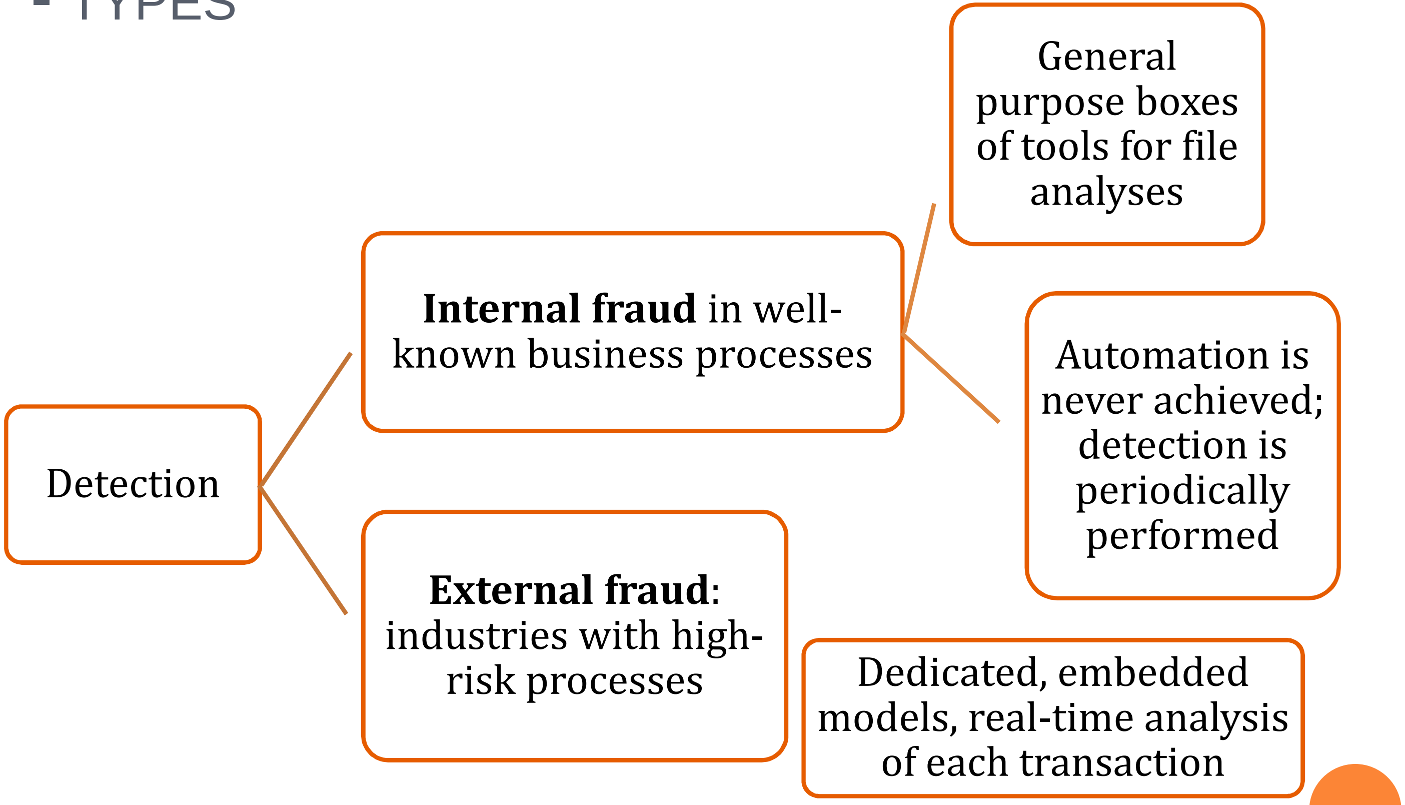
Analysis can also be made on the effectiveness of established controls through cost / benefit analysis both pre- and post-implementation of fraud controls.



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



Detection

Internal fraud in well-known business processes

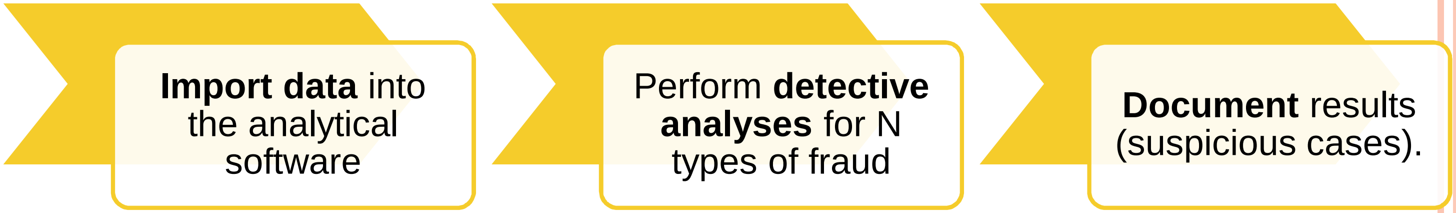
General purpose boxes of tools for file analyses

Automation is never achieved; detection is periodically performed

External fraud: industries with high-risk processes

Dedicated, embedded models, real-time analysis of each transaction

IS for fraud detection - Internal



Import data into the analytical software

Perform **detective analyses** for N types of fraud

Document results (suspicious cases).

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

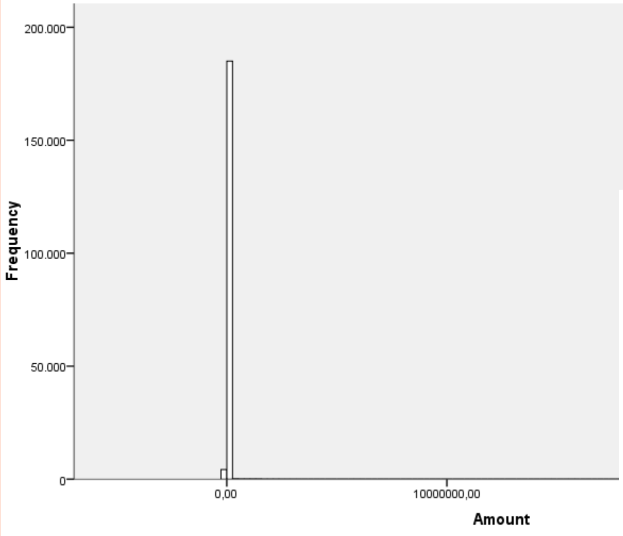
- Look for duplicate payments made fraudulently by an employee in collusion with a vendor.
- Look for duplicate purchases made using payment- or credit-cards within a short time. One of the purchases may be for personal use.
- Compare recent and previous versions of master files of the entity’s ERP database 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

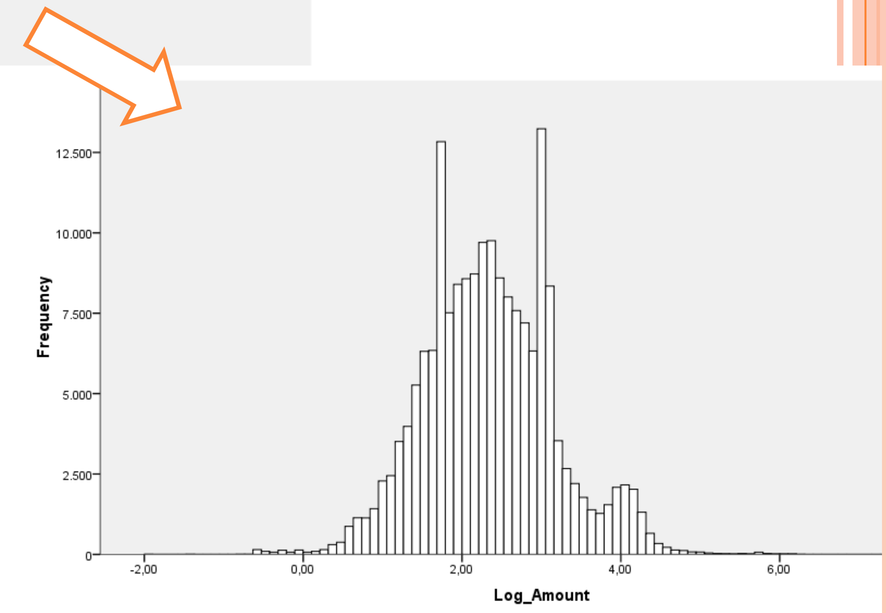
- Non-authorized expenses: examine dates (weekend purchases are suspect), vendor code or purchase description. Split transactions are also suspect.
- Compare suppliers' and payments' data with human resources records to search for "phantom vendors" set by employees to their advantage. Some type of **loose 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



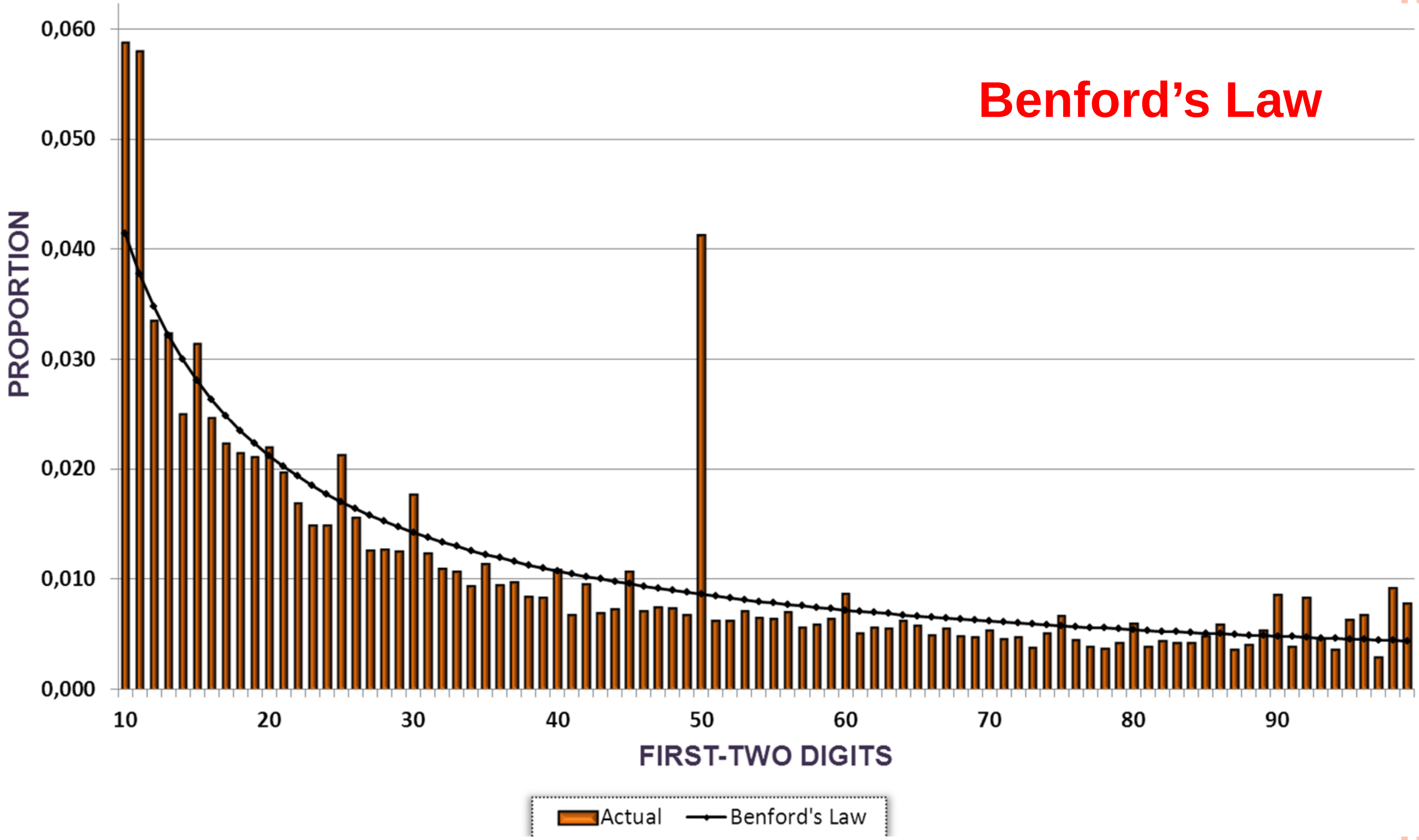
Calculated field: Logarithmic axis for money amounts



IS FOR FRAUD DETECTION - INTERNAL - TOOLS 2

Tool	Description
Benford’s Law	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.
Duplicates	Identifies duplicate items within a specified field in a file: identify duplicate billings of invoices and others.
Export	Creates a file in different software format: Excel, Word. Export customer address information to Word for “Mail Merging to customer confirmation letters.

IS FOR FRAUD DETECTION - INTERNAL - TOOLS 2



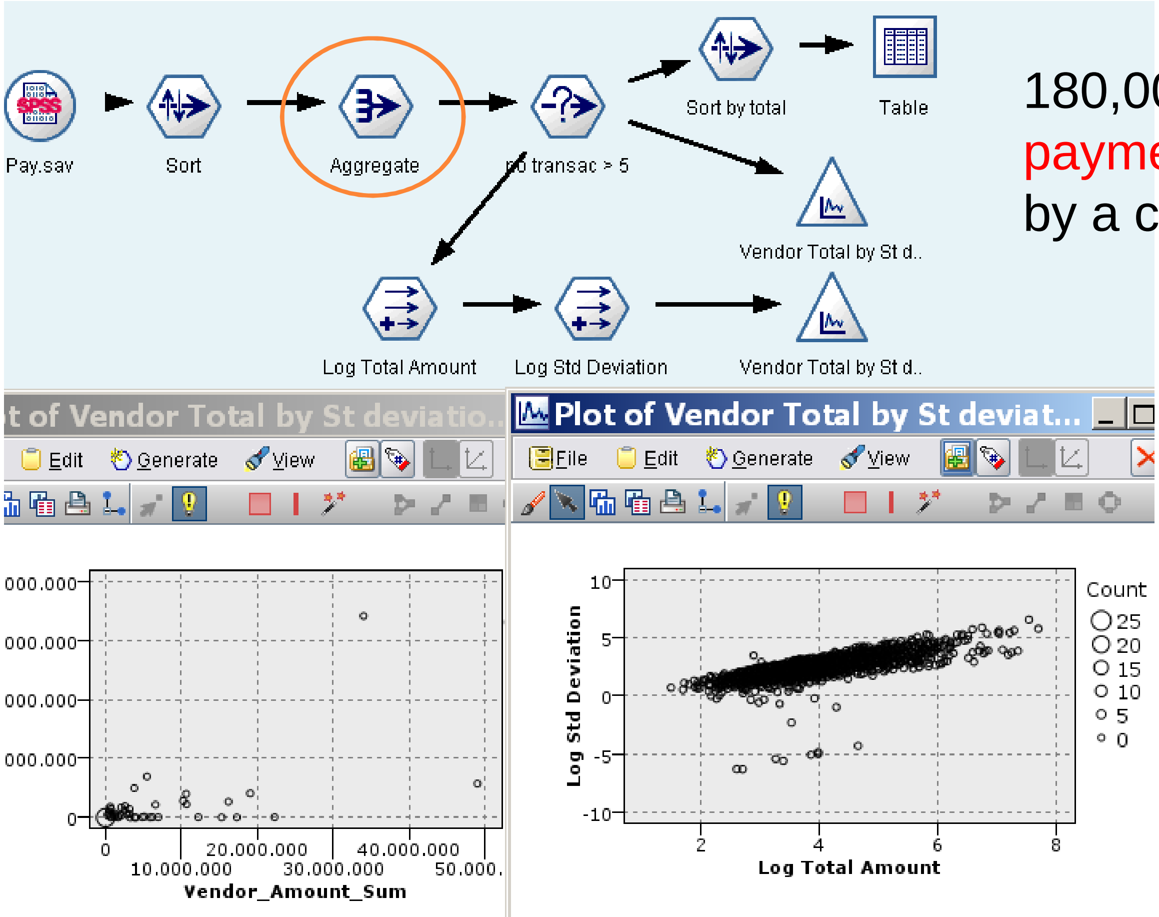
IS FOR FRAUD DETECTION - INTERNAL - TOOLS 3

Tool	Description
Extract / Filter	Extracts specified items from one file and copies them to another file, normally using “if” statement.
Gaps	Identifies gaps within a specified field in a file: identify any gaps in check sequence or others.
Index / Sort	Sorts a file in ascending or descending order: sorting a file by social security number to see if any blank or “99999” numbers exist.
Join / Relate	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.

IS for fraud detection - Internal - Tools 4

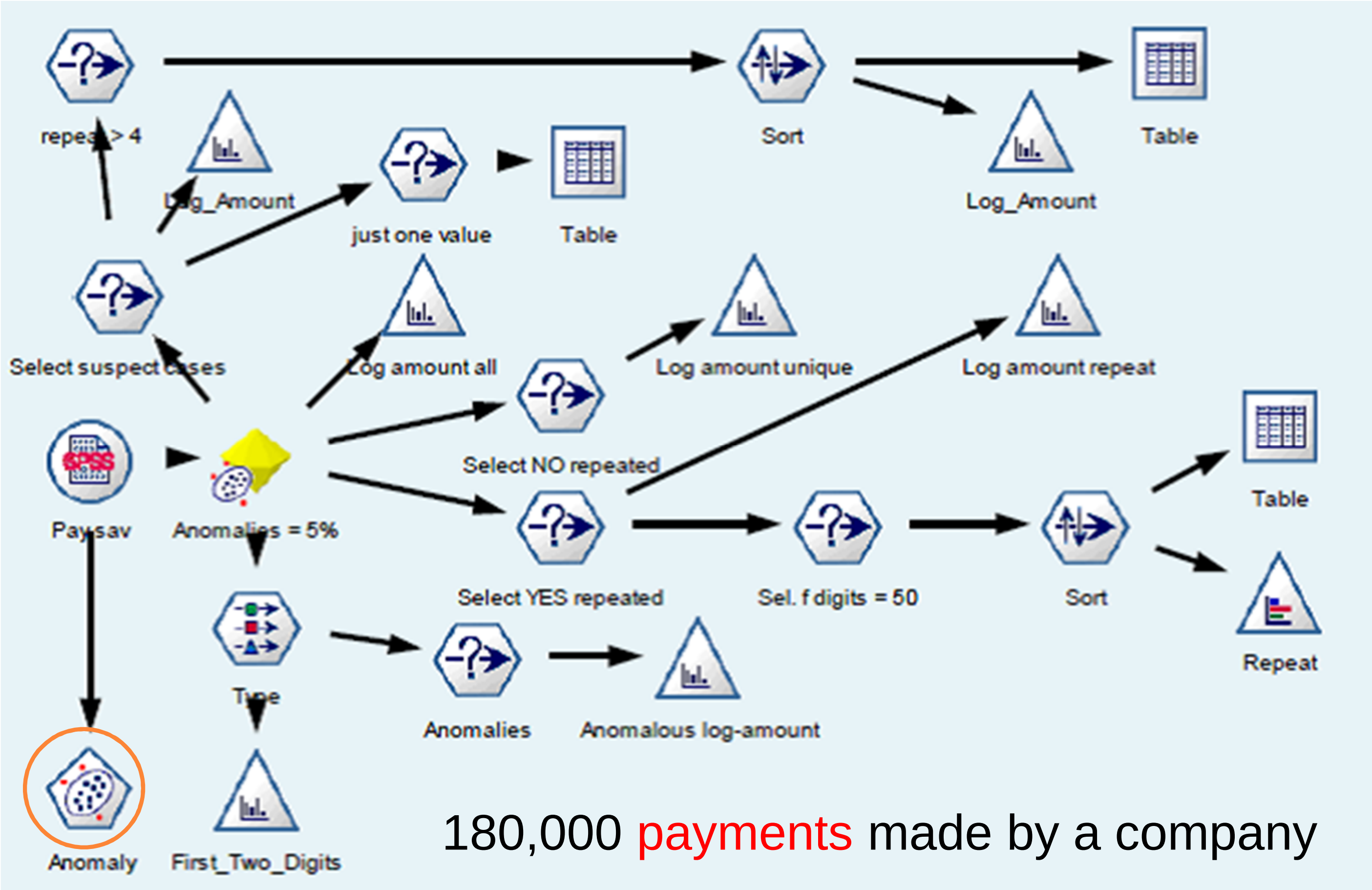
Tools	Description
Regression	Calculates a variable balance such as net sales based on other related variables: product purchases, inventory, etc.
Sample	Creates random or monetary unit samples from a specified population.
Statistics	Calculates statistics on a selected numeric field: total positive items,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

IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 1



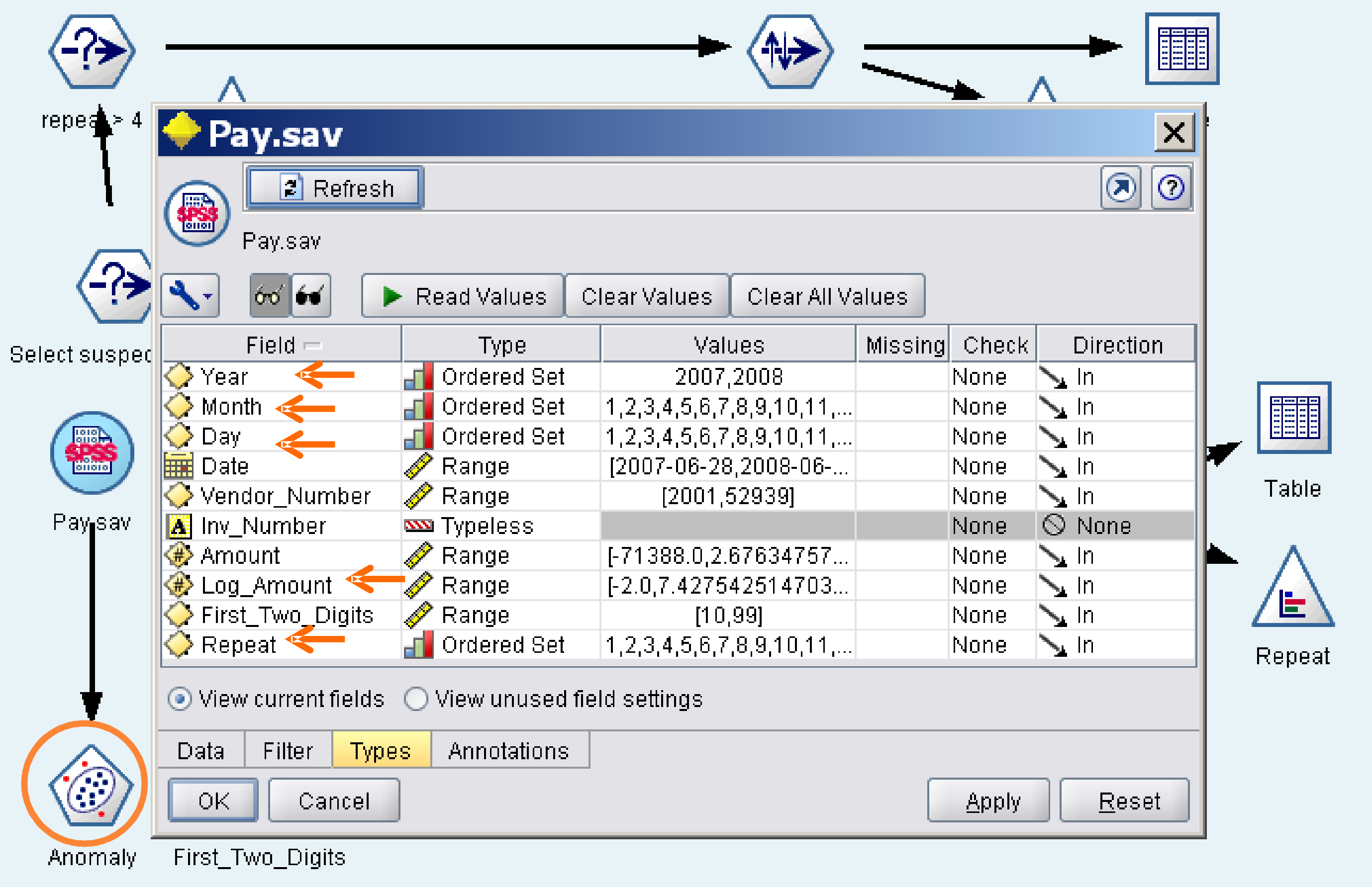
180,000 payments made by a company

IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2



180,000 payments made by a company

IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2

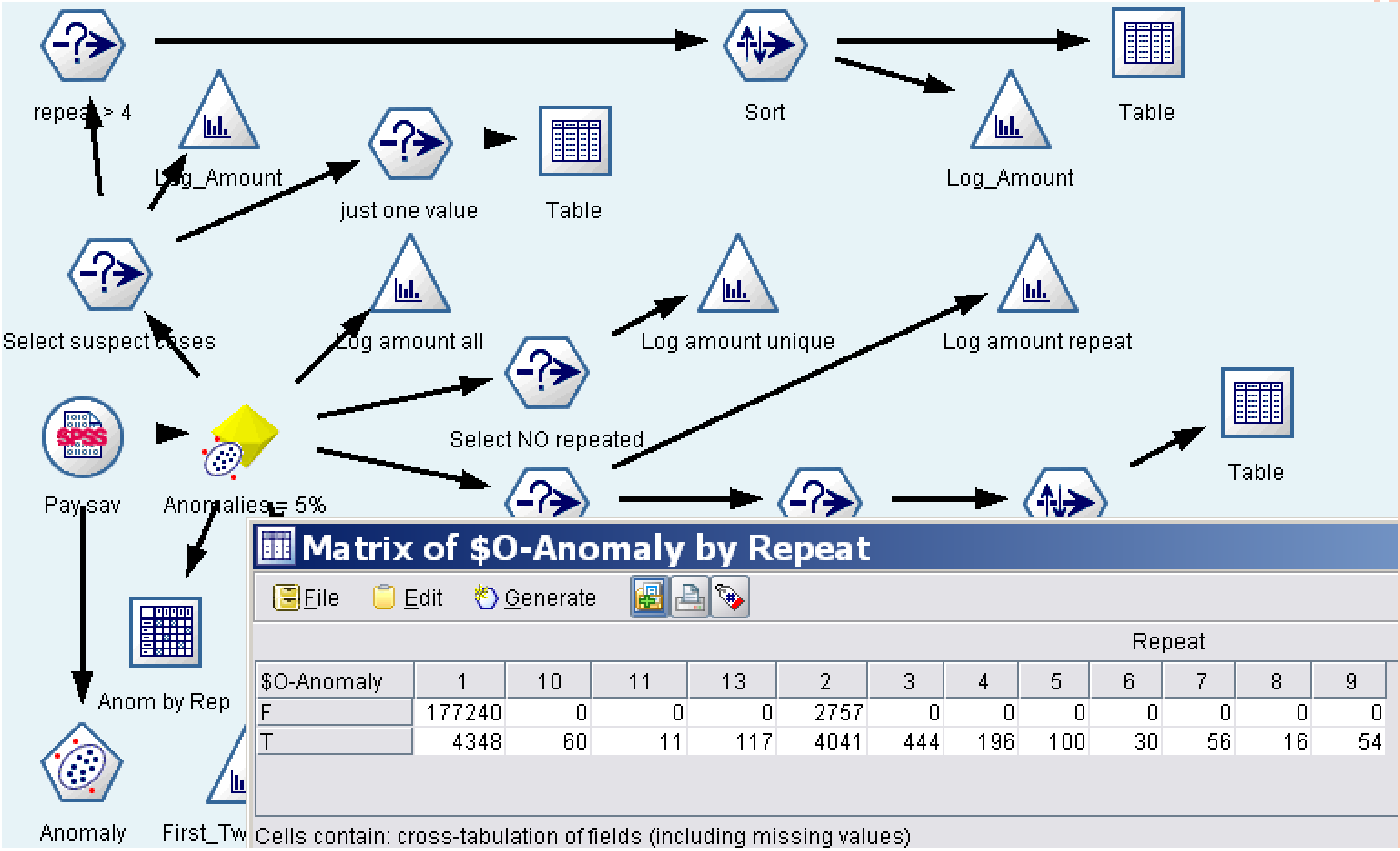


Pay.sav

Field	Type	Values	Missing	Check	Direction
Year	Ordered Set	2007,2008		None	In
Month	Ordered Set	1,2,3,4,5,6,7,8,9,10,11,...		None	In
Day	Ordered Set	1,2,3,4,5,6,7,8,9,10,11,...		None	In
Date	Range	[2007-06-28,2008-06-...		None	In
Vendor_Number	Range	[2001,52939]		None	In
Inv_Number	Typeless			None	None
Amount	Range	[-71388.0,2.67634757...		None	In
Log_Amount	Range	[-2.0,7.427542514703...		None	In
First_Two_Digits	Range	[10,99]		None	In
Repeat	Ordered Set	1,2,3,4,5,6,7,8,9,10,11,...		None	In

● View current fields ○ View unused field settings

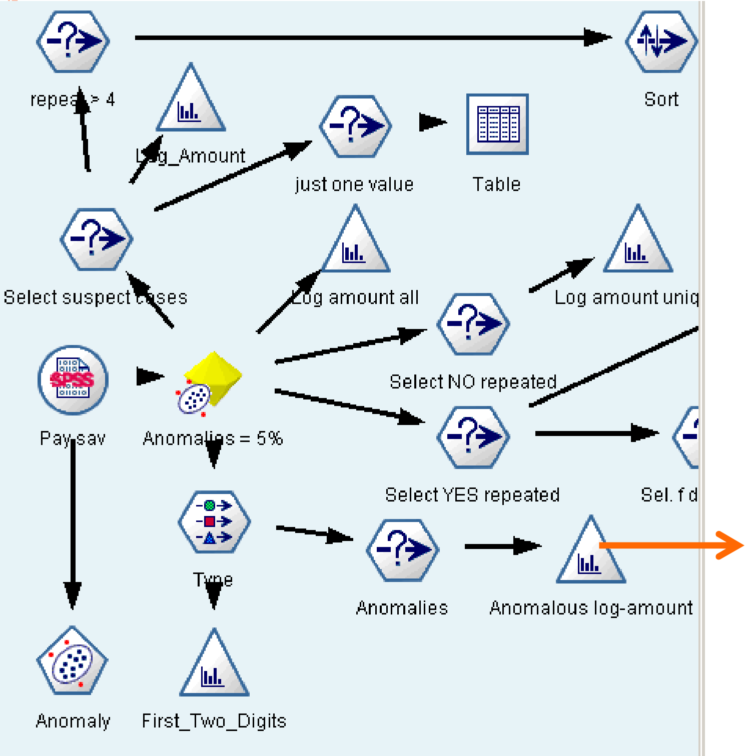
IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2

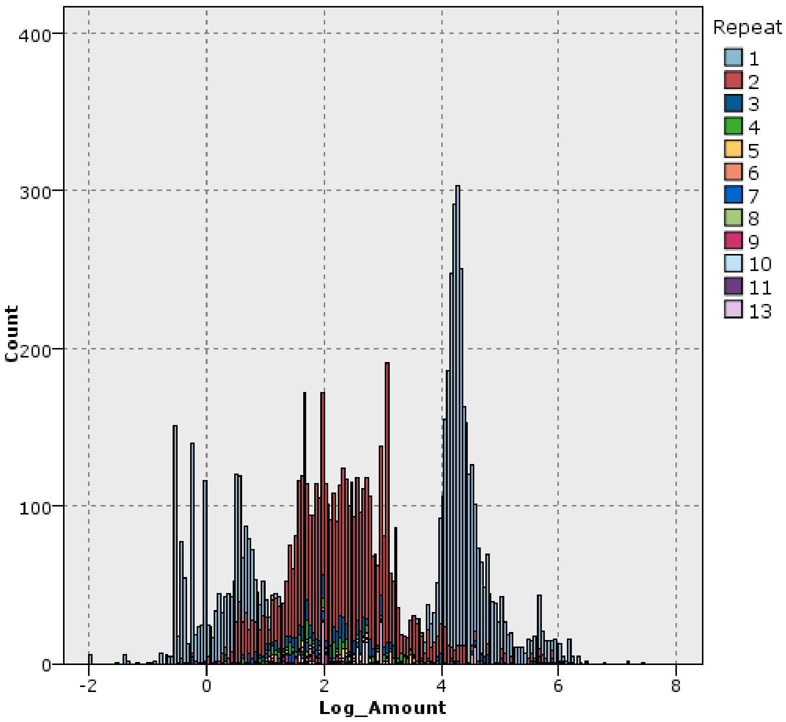


	Repeat											
$O-Anomaly	1	10	11	13	2	3	4	5	6	7	8	9
F	177240	0	0	0	2757	0	0	0	0	0	0	0
T	4348	60	11	117	4041	444	196	100	30	56	16	54

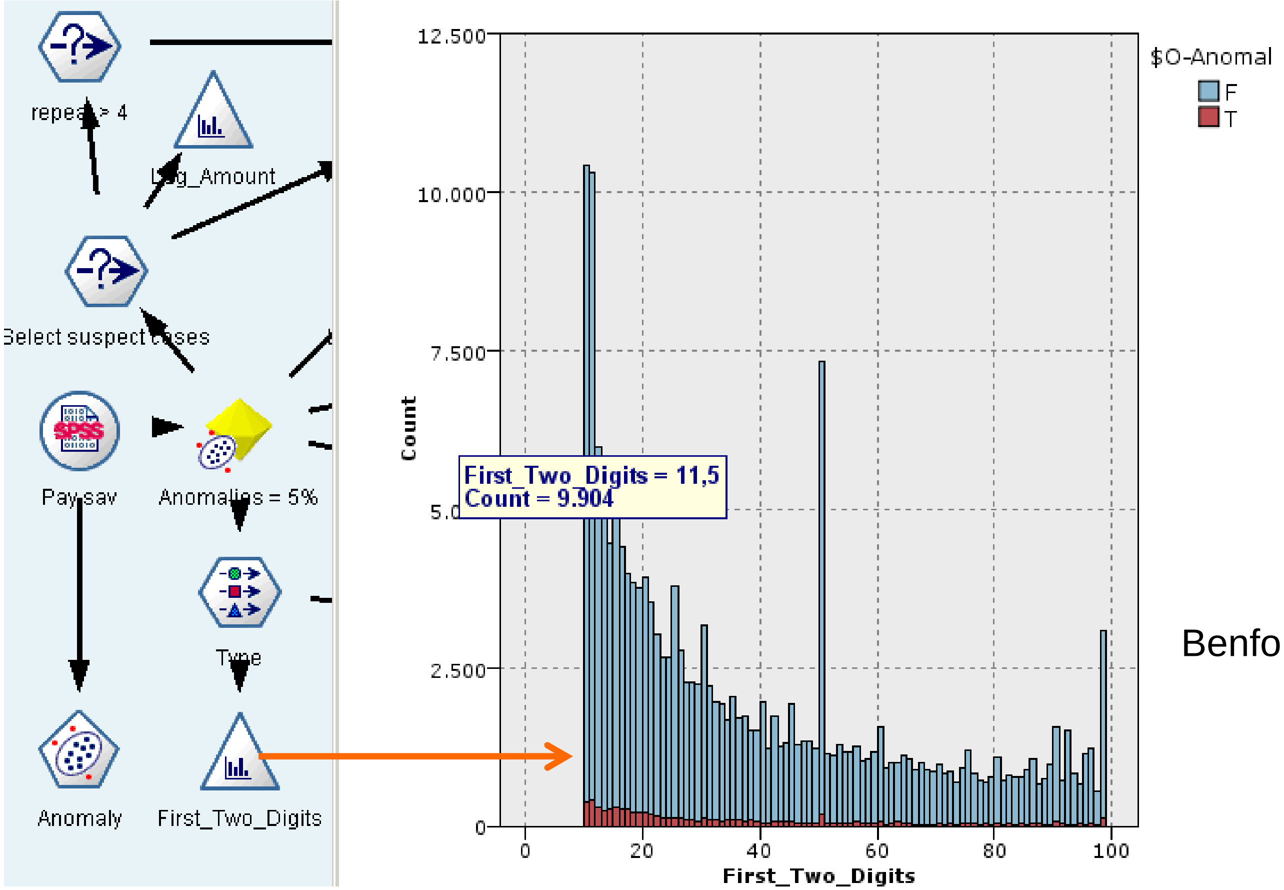
Cells contain: cross-tabulation of fields (including missing values)

IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2



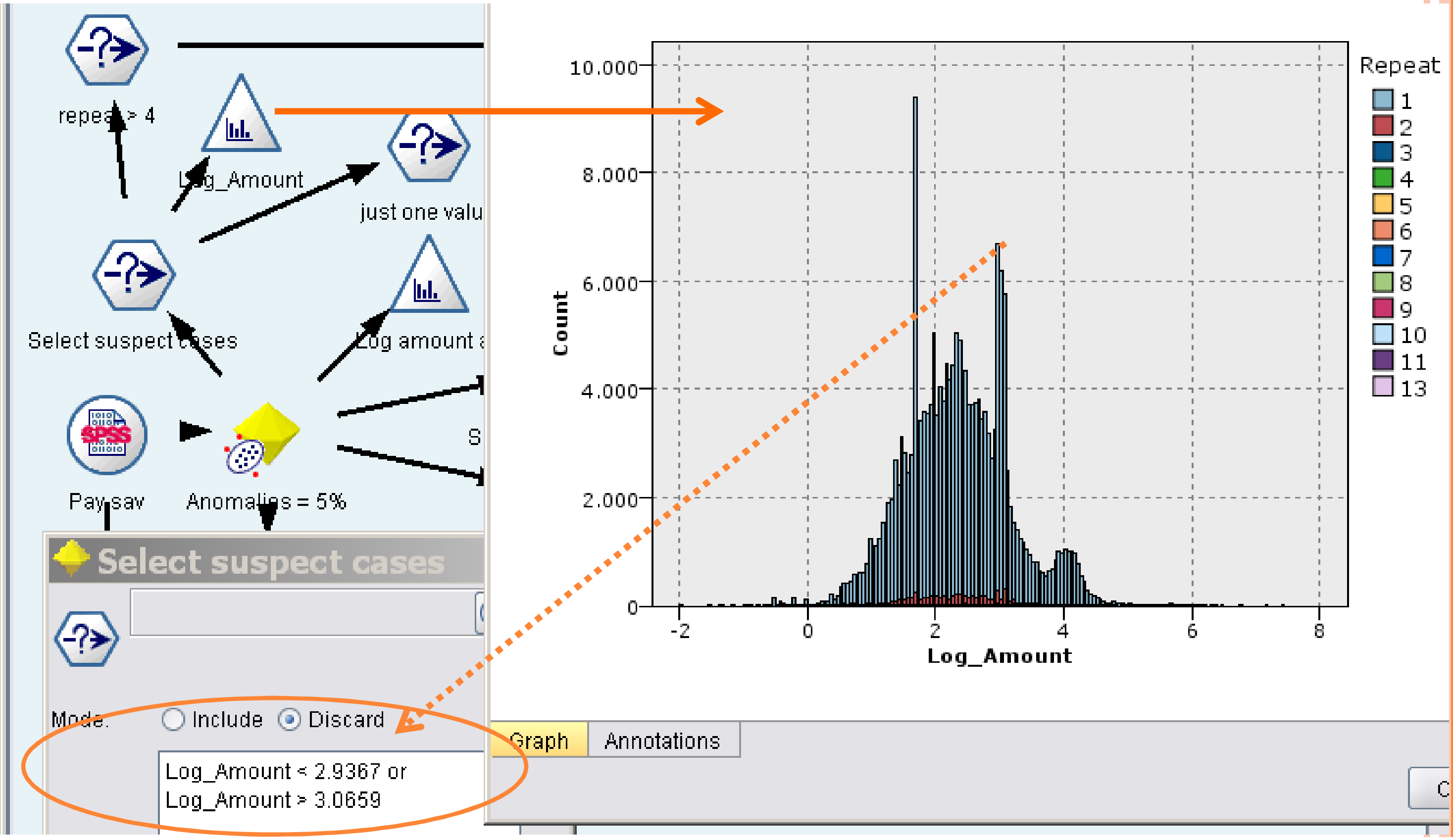


IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2



Benford’s

IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2



Mode: ○ Include ● Discard

Log_Amount < 2.9367 or
Log_Amount > 3.0659

IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2

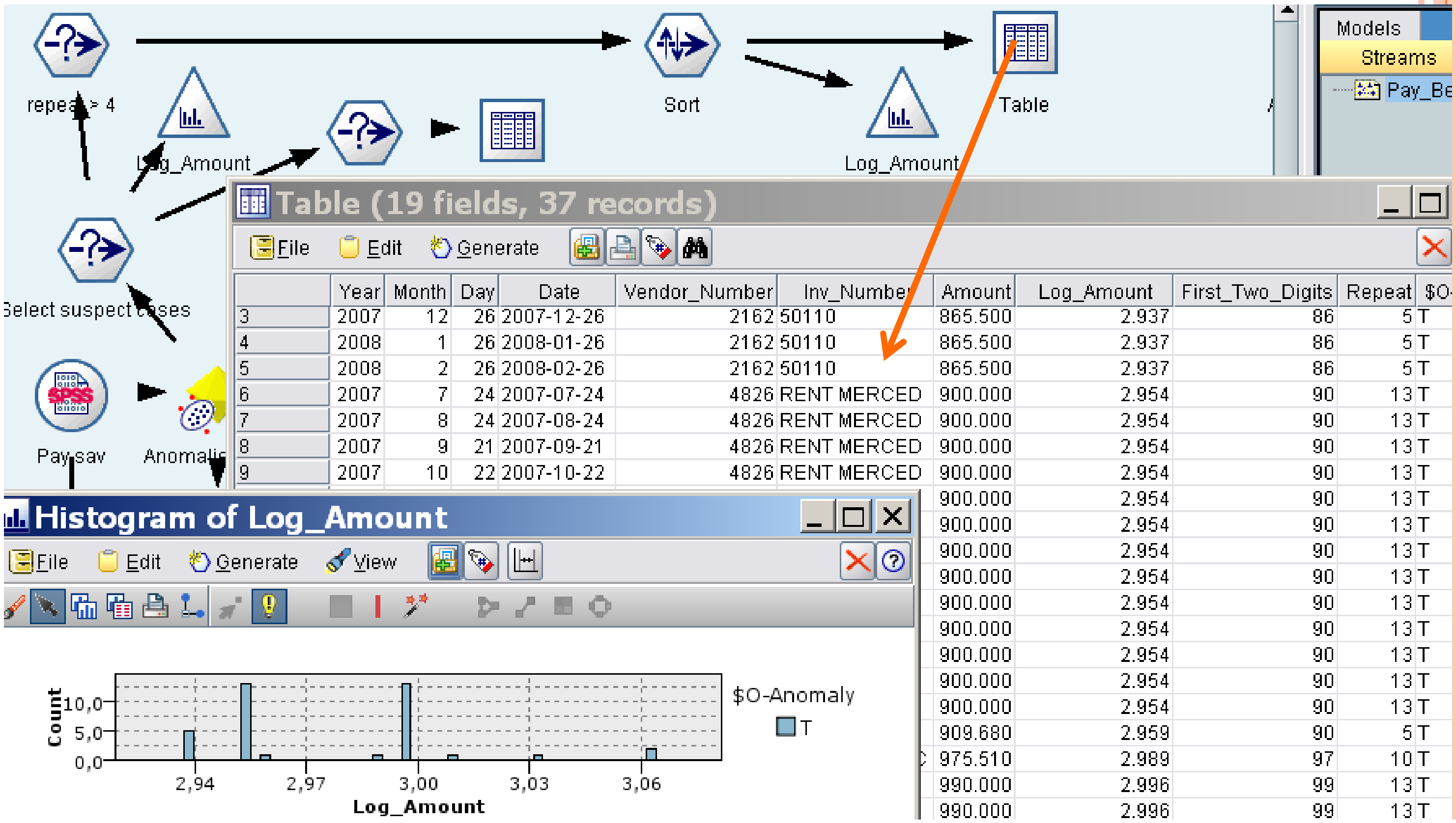
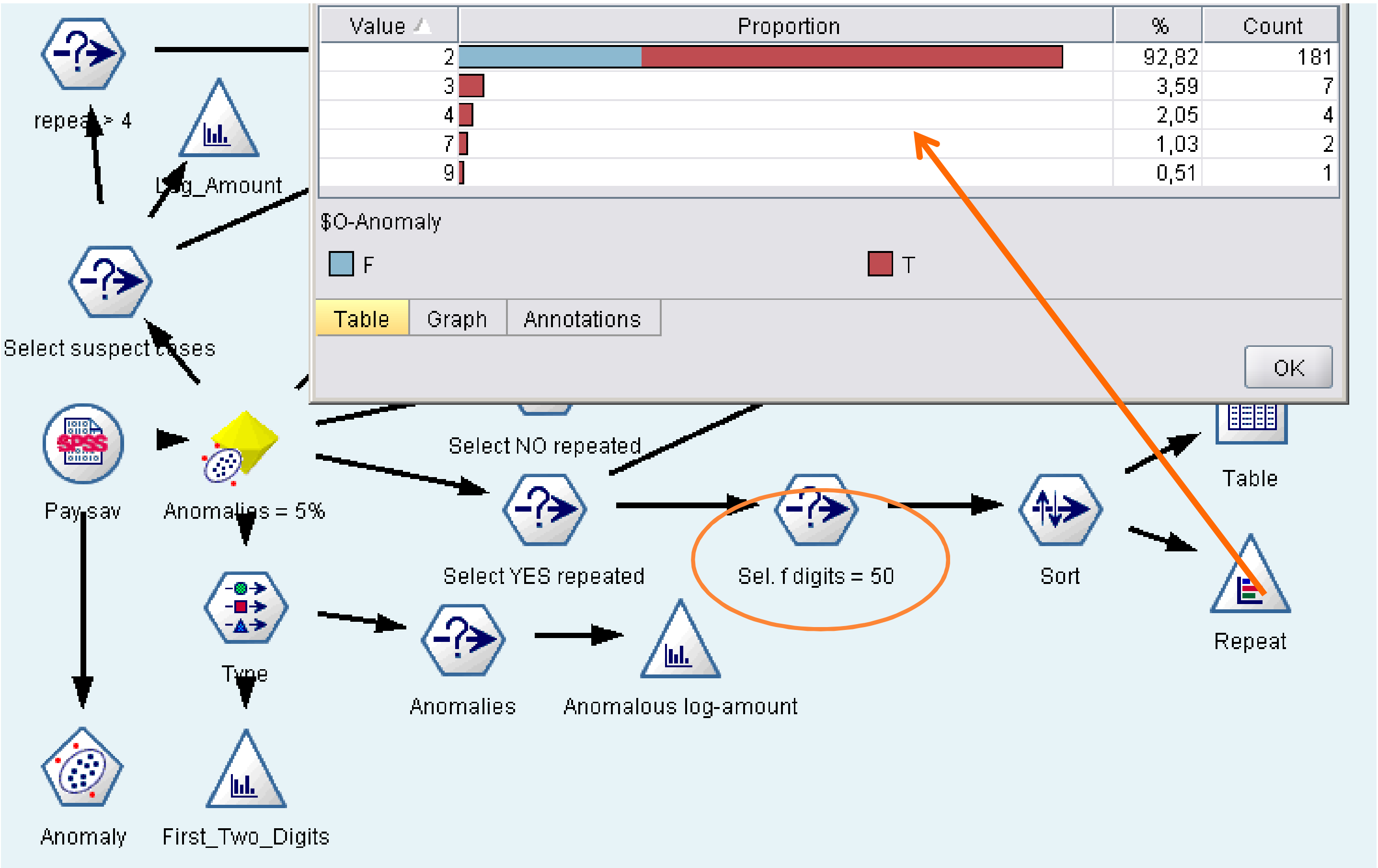


Table (19 fields, 37 records)

File Edit Generate

	Year	Month	Day	Date	Vendor_Number	Inv_Number	Amount	Log_Amount	First_Two_Digits	Repeat	$O-
3	2007	12	26	2007-12-26	2162	50110	865.500	2.937	86	5	T
4	2008	1	26	2008-01-26	2162	50110	865.500	2.937	86	5	T
5	2008	2	26	2008-02-26	2162	50110	865.500	2.937	86	5	T
6	2007	7	24	2007-07-24	4826	RENT MERCED	900.000	2.954	90	13	T
7	2007	8	24	2007-08-24	4826	RENT MERCED	900.000	2.954	90	13	T
8	2007	9	21	2007-09-21	4826	RENT MERCED	900.000	2.954	90	13	T
9	2007	10	22	2007-10-22	4826	RENT MERCED	900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							900.000	2.954	90	13	T
							909.680	2.959	90	5	T
							975.510	2.989	97	10	T
							990.000	2.996	99	13	T
							990.000	2.996	99	13	T

IS FOR FRAUD DETECTION
- INTERNAL – EXAMPLE 2

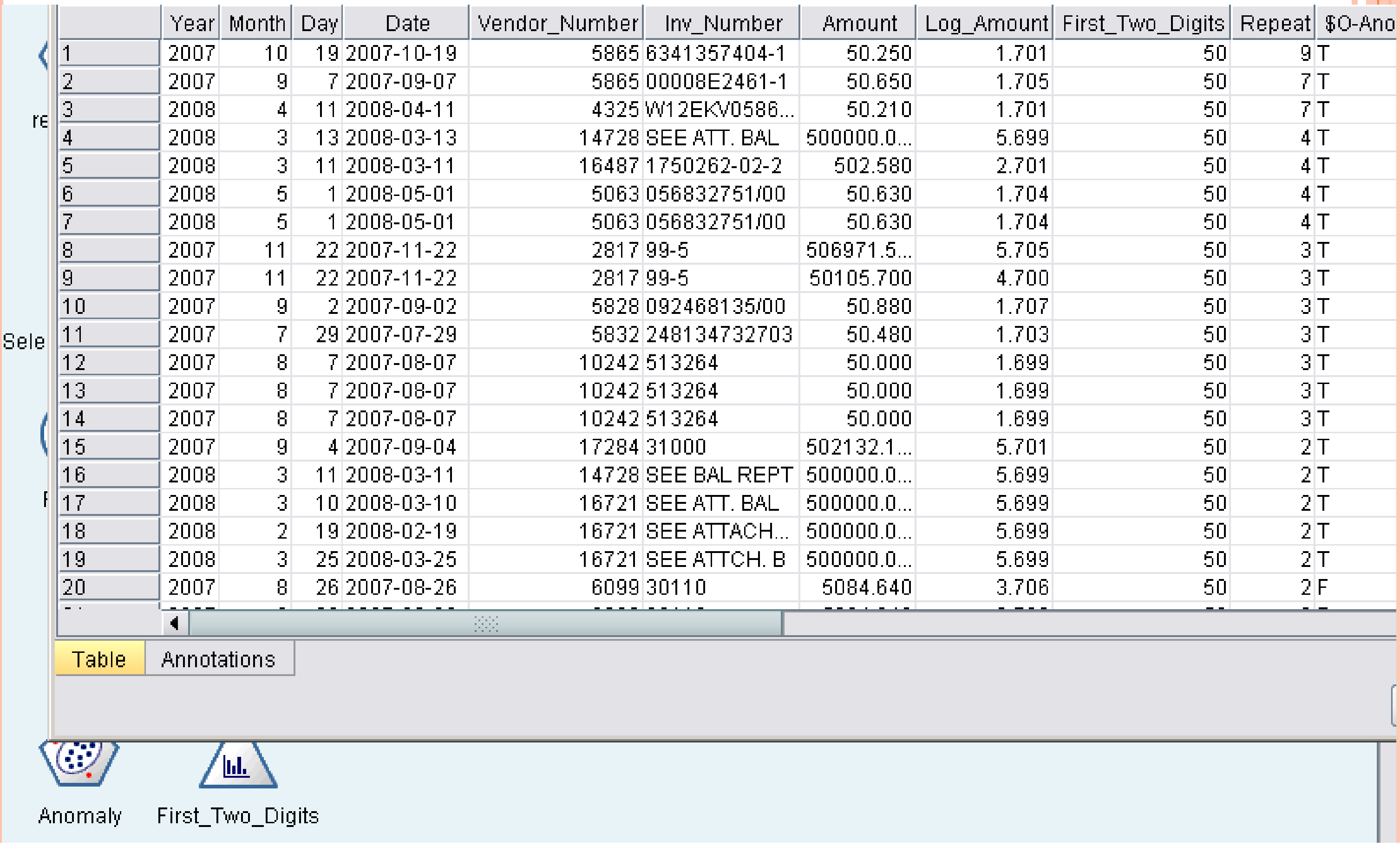


Value	Proportion	%	Count
2		92,82	181
3		3,59	7
4		2,05	4
7		1,03	2
9		0,51	1

$O-Anomaly

🟦 F 🟥 T

IS FOR FRAUD DETECTION - INTERNAL – EXAMPLE 2



	Year	Month	Day	Date	Vendor_Number	Inv_Number	Amount	Log_Amount	First_Two_Digits	Repeat	$O-Ano
1	2007	10	19	2007-10-19	5865	6341357404-1	50.250	1.701	50	9	T
2	2007	9	7	2007-09-07	5865	00008E2461-1	50.650	1.705	50	7	T
3	2008	4	11	2008-04-11	4325	W12EKV0586...	50.210	1.701	50	7	T
4	2008	3	13	2008-03-13	14728	SEE ATT. BAL	500000.0...	5.699	50	4	T
5	2008	3	11	2008-03-11	16487	1750262-02-2	502.580	2.701	50	4	T
6	2008	5	1	2008-05-01	5063	056832751/00	50.630	1.704	50	4	T
7	2008	5	1	2008-05-01	5063	056832751/00	50.630	1.704	50	4	T
8	2007	11	22	2007-11-22	2817	99-5	506971.5...	5.705	50	3	T
9	2007	11	22	2007-11-22	2817	99-5	50105.700	4.700	50	3	T
10	2007	9	2	2007-09-02	5828	092468135/00	50.880	1.707	50	3	T
11	2007	7	29	2007-07-29	5832	248134732703	50.480	1.703	50	3	T
12	2007	8	7	2007-08-07	10242	513264	50.000	1.699	50	3	T
13	2007	8	7	2007-08-07	10242	513264	50.000	1.699	50	3	T
14	2007	8	7	2007-08-07	10242	513264	50.000	1.699	50	3	T
15	2007	9	4	2007-09-04	17284	31000	502132.1...	5.701	50	2	T
16	2008	3	11	2008-03-11	14728	SEE BAL REPT	500000.0...	5.699	50	2	T
17	2008	3	10	2008-03-10	16721	SEE ATT. BAL	500000.0...	5.699	50	2	T
18	2008	2	19	2008-02-19	16721	SEE ATTACH...	500000.0...	5.699	50	2	T
19	2008	3	25	2008-03-25	16721	SEE ATTCH. B	500000.0...	5.699	50	2	T
20	2007	8	26	2007-08-26	6099	30110	5084.640	3.706	50	2	F

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

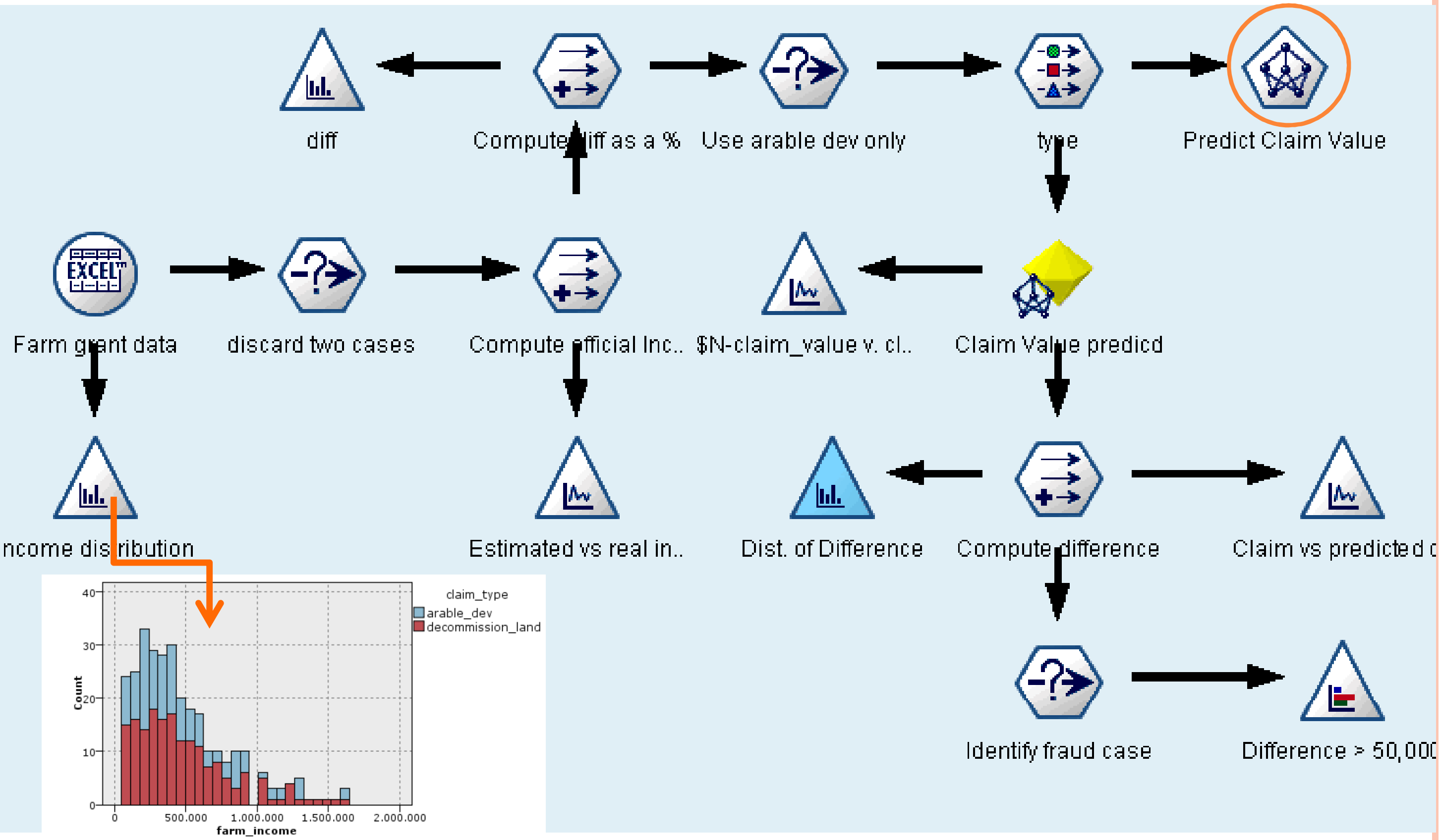
- Insurance and Government – fraudulent claims,
- Bank loan application – false statement
- Healthcare false billings,
- Retail post-of-sale or Internet and others

… identity theft underlies several such frauds

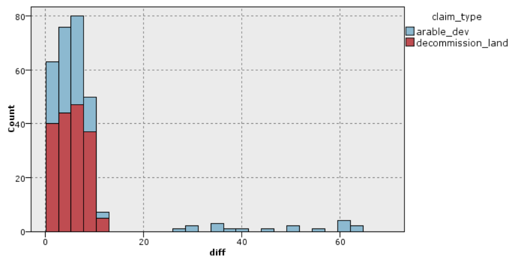
EXAMPLE: fraud in claims of farm subsidies:

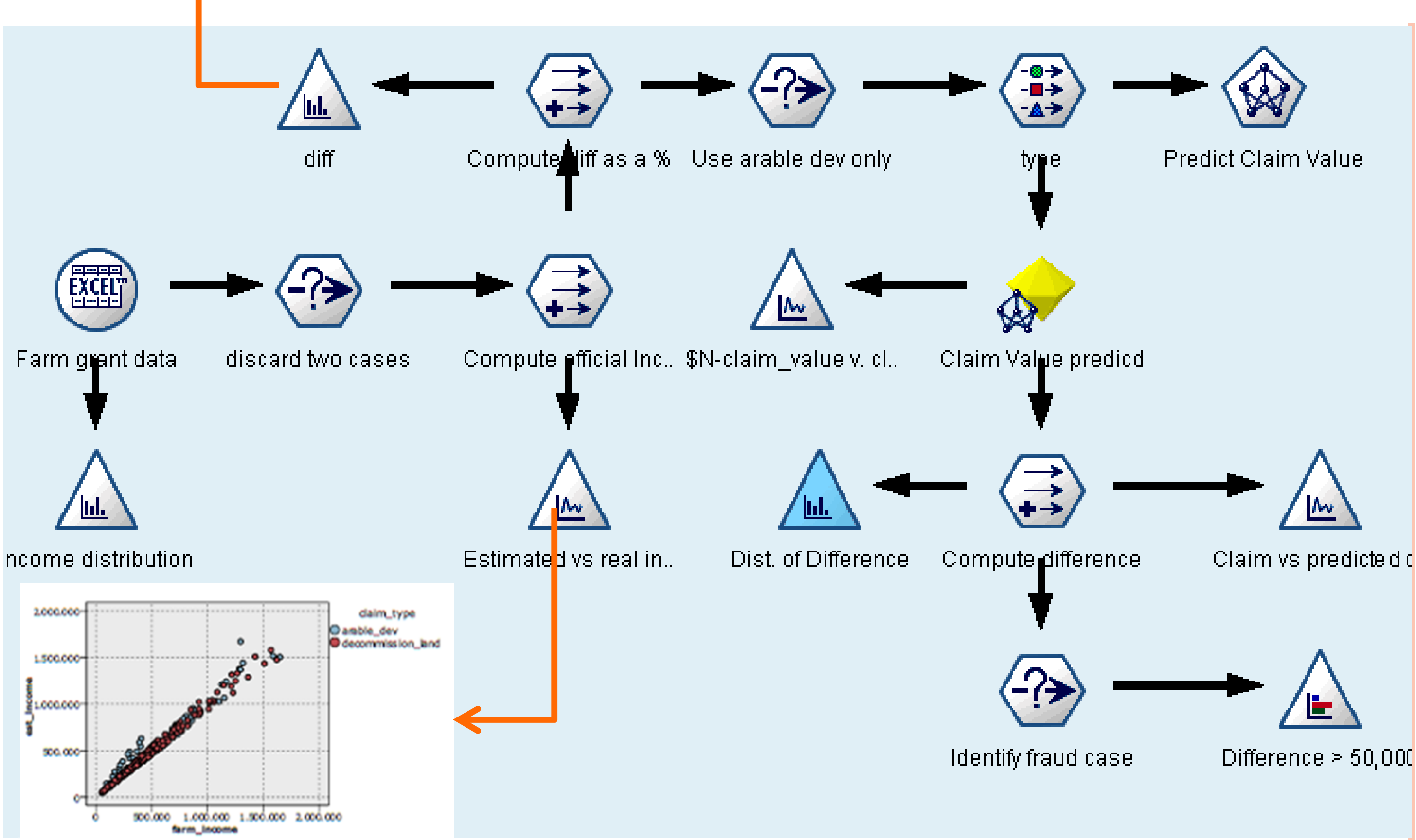
id	region	farm size	rain fall	land quality	farm income	main crop	claim type	claim value
id601	midlands	1480	30	8	330729	wheat	decommission_land	74703,1
id602	north	1780	42	9	734118	maize	arable_dev	245354
id605	north	1700	46	8	621148	wheat	decommission_land	122006
id606	southeast	1580	42	7	445785	maize	arable_dev	122135
. . .	… total of 298 claims							

IS FOR FRAUD DETECTION - EXTERNAL - EXAMPLE

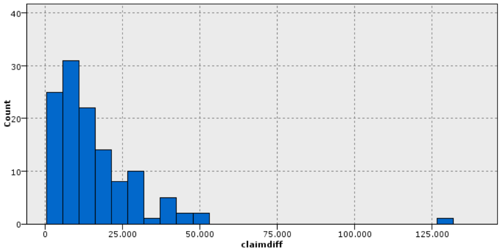


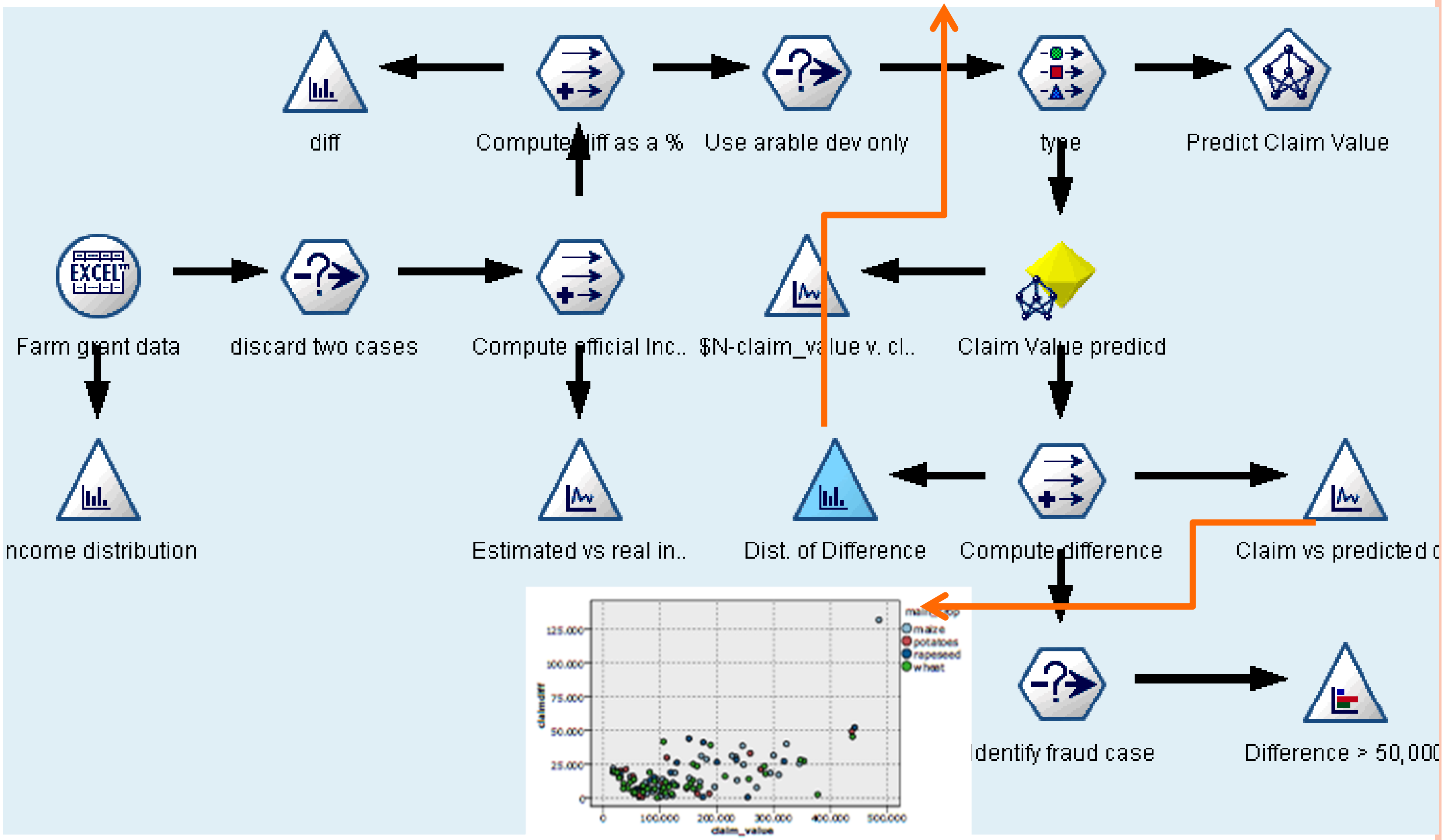
IS FOR FRAUD DETECTION - EXTERNAL - EXAMPLE





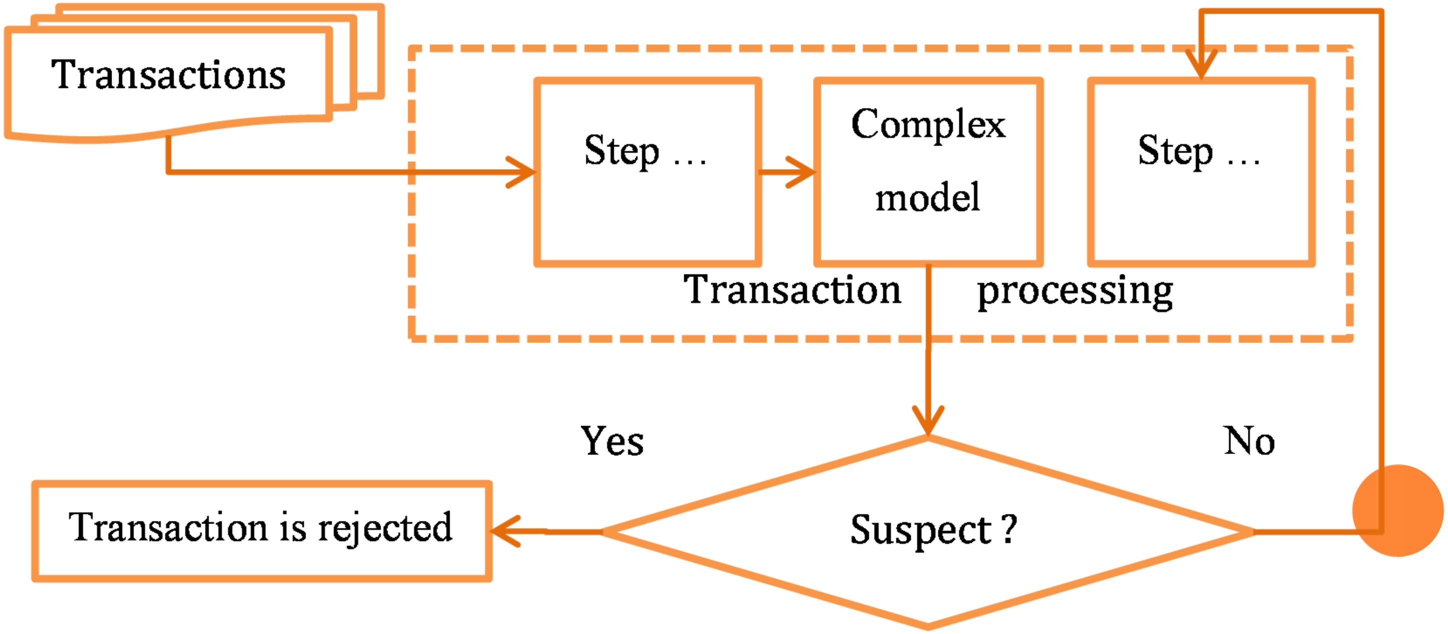
IS for fraud detection - External - example





IS FOR FRAUD DETECTION - EXTERNAL - TASK

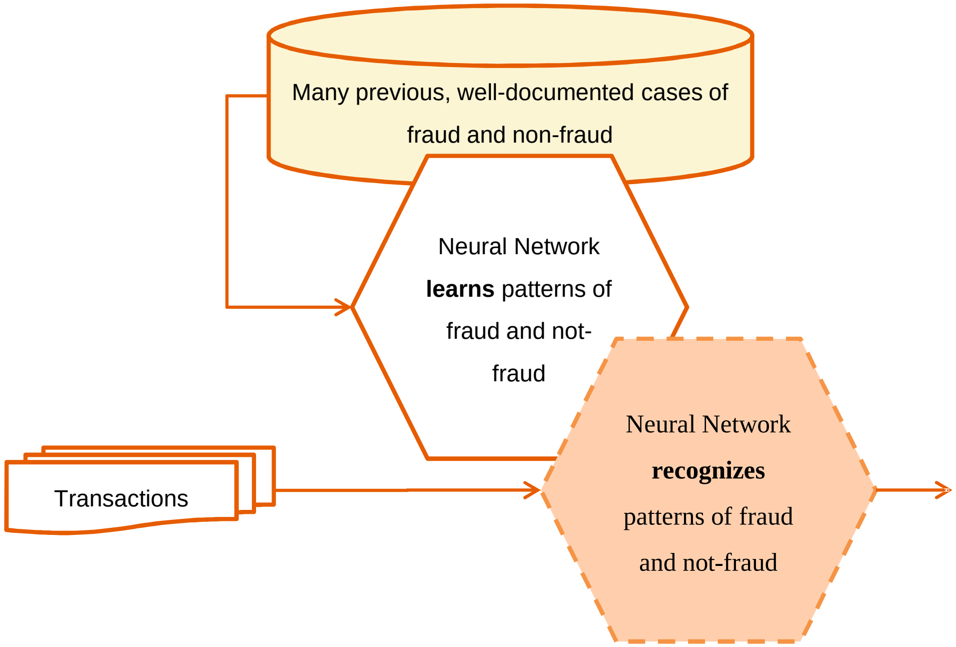
Detection is carried out in real time, embedding in the transaction processing software, one or several complex models able to check the plausibility of transactions:



IS FOR FRAUD DETECTION - EXTERNAL - TASK

Complex models

1. **learn** fraud patterns from previous, detected cases
2. **recognize** transactions where such pattern is present


Many previous, well-documented cases of fraud and non-fraud
Neural Network **learns** patterns of fraud and not-fraud
Transactions
Neural Network **recognizes** patterns of fraud and not-fraud

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

- IBM Counter Fraud Management (for Banking, healthcare, Insurance, Government) http://www-03.ibm.com/security/counter-fraud/solution/index.html
- ACL may detect external fraud through continuous transaction analysis in, for example, SAP software http://www.acl.com/solutions/products/acl-direct-link/
- SAS Institute, SAS security intelligence http://www.sas.com/en_us/software/fraud-security-intelligence.html stand-alone solutions that work with several transaction processing software.
- ORACLE (Financial Services division) fraud-detecting models embedded in transaction-processing products http://www.oracle.com/us/products/applications/financial-services/fraud/index.html
- SAP has native fraud detection models embedded in transaction-processing products http://www.sap.com

SOURCES AND REFERENCES

- "A Guide to forensic accounting investigation", T. W. Golden *et al*., Wiley, 2006.
- "Managing the business risk of fraud: a practical guide", AICPA and ACFE, url: https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf
- "Fraud Control in Australian Government Entities: Better Practice Guide", Australian National Audit Office and KPMG, March 2011, url: https://www.anao.gov.au/sites/g/files/net616/f/2011_Fraud_Control_BPG.pdf
- "Fraud data interrogation tools: comparing best software for fraud examinations", Rich Lanza, Fraud Magazine, url: http://www.fraud-magazine.com/article.aspx?id=4294967837