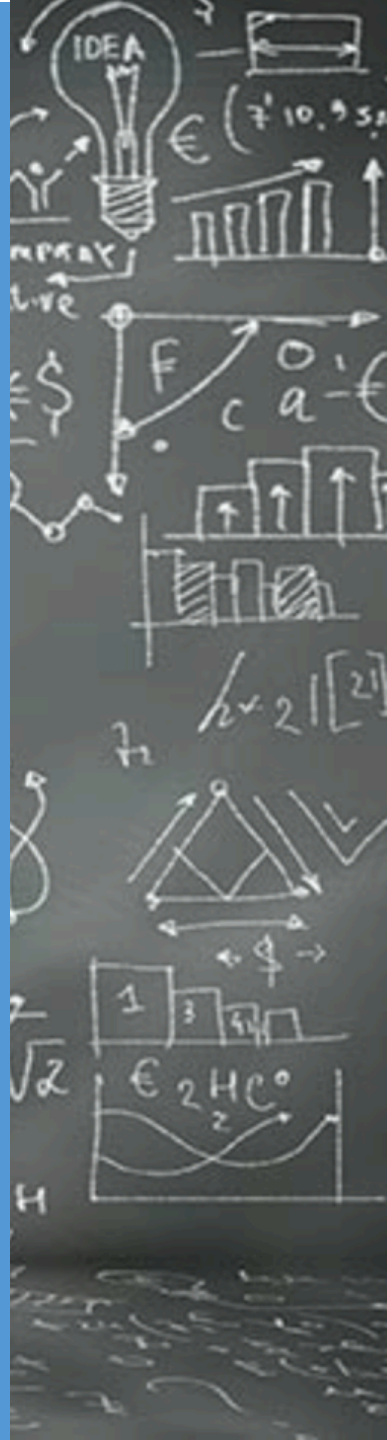
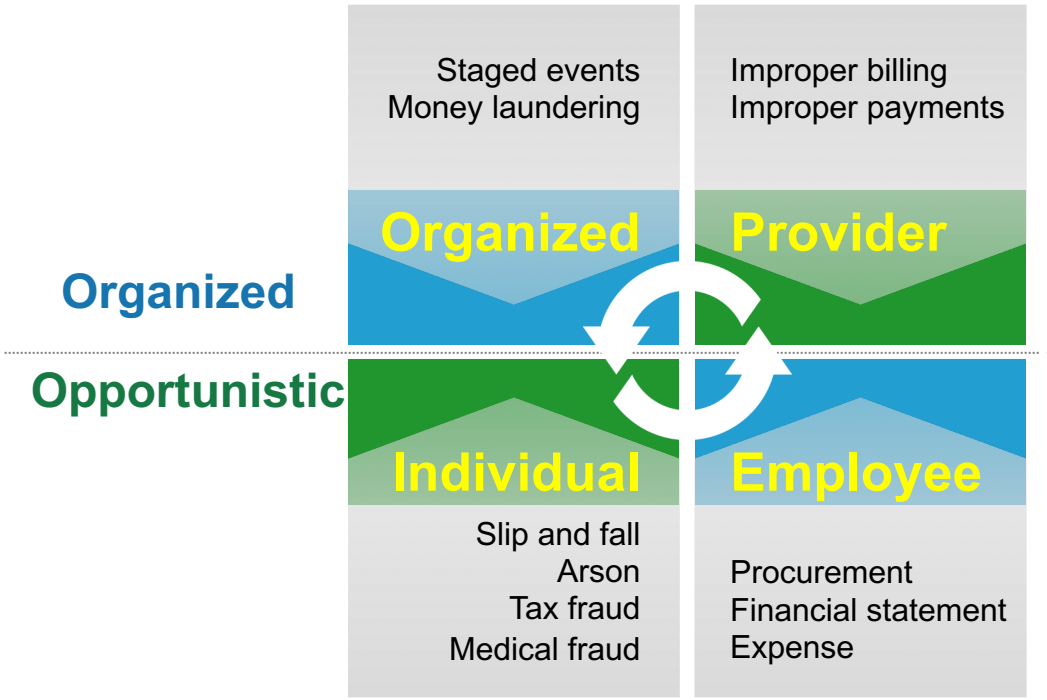
Risk and Fraud Management

Yann Gouedo
Data Scientist Leader – Machine Learning / Artificial Intelligence
Marketing / Risk / Fraud / Maintenance
IBM Certified Senior Data Scientist & IBM Certified Senior Architect



Fraud is a deliberate deception or misrepresentation which violates a legal statute and is intended to produce an undue financial gain



Scope includes

Financial crime including money laundering, cyber attack and illegal security breach.

Abuse which similar to fraud but not determined to violate the law.

Waste & Error refer to improper payments which are the result of over paying due to poor policies or operational mistakes

Risk includes financial, operational, IT and security risks and financial crimes which all must be identified, monitored and controlled.

Four capabilities are needed to defeat Fraudsters

Counter Fraud Solution Framework

Operational Systems

Advanced Industry Libraries:
Data Models, Predictive Models, Rules, Reports, Process, External Fraud Data and so on

Real Time / "In line"

Back Office Analytics

Prevention

Integration

Action

Guidance

Rules

Detection

Predictive Analytics

Rules

Decision Management

Discovery

Selection

Evaluation

Anomalies

Identification

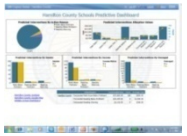
Investigation

Case Management

Relationship Visualization

Investigative Analytics

Reporting



Operational Reporting

Dashboards

Feedback

Observation Space

Information Domains

Internal Sources

External Sources

Evolving Unstructured Sources

Fraud Use Case Libraries


CUSTOMER USE CASE

PRO BTP uses analytical tools for real-time detection of suspicious claims for medical expenses

Identified

9% of suspicious claims in optics and 14% in dental

14 million euros

is the potential damage over a period of 21 months

Reduced

management costs and improved service

Solution components

- IBM Fraud and Abuse Management System
- IBM Counter Fraud industry solution
- IBM® InfoSphere®
- IBM SPSS® Decision Management
- IBM WebSphere® Application Server
- IBM Operational Decision Manager
- IBM i2® Analyst's Notebook®
- IBM Global Business Services® – Consulting and Application Management Services
- IBM Global Technology Services® – Integrated Technology Services
- IBM PureFlex® System
- IBM Client Center at La Gaude

Business challenge: PRO BTP is the social protection group for French building and construction professionals. It offers members (employees, retirees, craftsmen and construction companies) services in the areas of pension and health insurance (provident, health and savings). The firm had been using a processing system that was identifying unjustified health claims only after they had been paid. To reduce system abuses and better control expenses, PRO BTP needed to detect suspicious claims before the company reimbursed health professionals.

The smarter solution: Teaming with PRO BTP, IBM developed a secure service platform dedicated to detecting, categorizing and fighting fraud, service abuses and errors. Thanks to a detection engine validated by experts, this service platform, named Solon, analyzes optical and dental reimbursement claims in real time so that the firm can evaluate them before payment or before establishing a charges agreement. The platform features enriched predictive models that it can use to help detect fraud networks, and it is based on self-learning technology that pools detection schemes and takes advantage of an observatory watch.

"We plan to extend the process to all of our health insurances, and eventually even to some provident benefits." —Paul Grasset, chief executive officer

A partnership between PROBTP and IBM for the creation of a counter fraud service

Customer 1

Customer 2

Customer 3

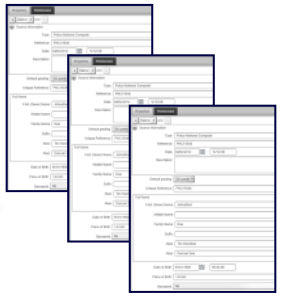
Customer 4

...

Customer n

PRO BTP GROUPE

IBM



- **Suspicious Request of reimbursment**
- **Health Practitioners Scoring**
- **Recommendations for the recovery and blocking payments**

Counter Fraud Solution Framework

Operational Systems

Advanced Industry Libraries:
Data Models, Predictive Models, Rules, Reports, Process, External Fraud Data and so on

Real Time / "In line"

Back Office Analytics

Prevention

Integration

Action

Guidance

Rules

Detection

Predictive Analytics

Rules

Decision Management

Discovery

Selection

Evaluation

Anomalies

Identification

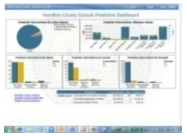
Investigation

Case Management

Relationship Visualization

Investigative Analytics

Reporting



Operational Reporting

Dashboards

Feedback

Observation Space

Information Domains

Internal Sources

External Sources

Evolving Unstructured Sources

Fraud Use Case Libraries

The Proof of Concept / Proof of Business: Business Value

First Findings - True stories based on 21 months of client's data

Identified
9% of optical and 14% of dental claims as suspicious cases in POC

Millions of euros
potentially saved in cost avoidance

50% of claims
scored as highly suspicious identified and validated

1 One beneficiary who "bought" **26 glasses**

2 A network fraud between a beneficiary and his **wife** who was …. **dental assistant**!

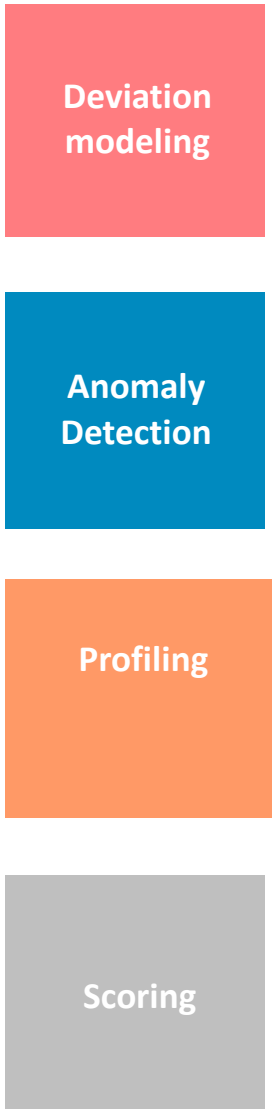
3 Many cases where we saw more than **8 dental prosthesis** for kids under the age of 15 years old

4 Contact lens for children under the age of **10 years** old

5 Many claims for the same practitioner → **Services not performed** /delivered has been billed (medical care, glasses, lens…)

6 Huge number of claims in the same month for the same practitioner (end of the year)

PoB's Fraud detection methodologies



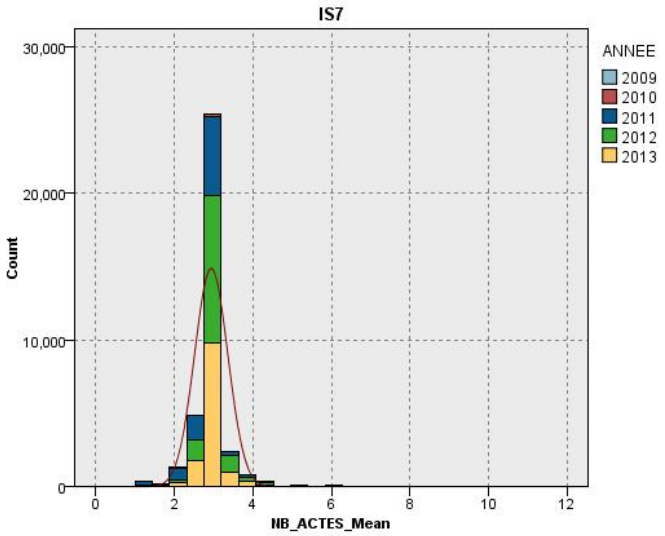
1) The first approach works by **apply business rules helping to detect suspicious cases, tuned with statistical information (mean, standart deviation, ….)**
2) The second approach works by **finding anomalies in behavior that could indicate fraud**
3) The third approach is based on **known business rules and indicators** and **creates suspicious cases scores / profiles of Practitioners**
4) *The fourth* approach *is based on* ***known fraudulent cases*** *et creates* ***fraud patterns*** *to apply on new claims*

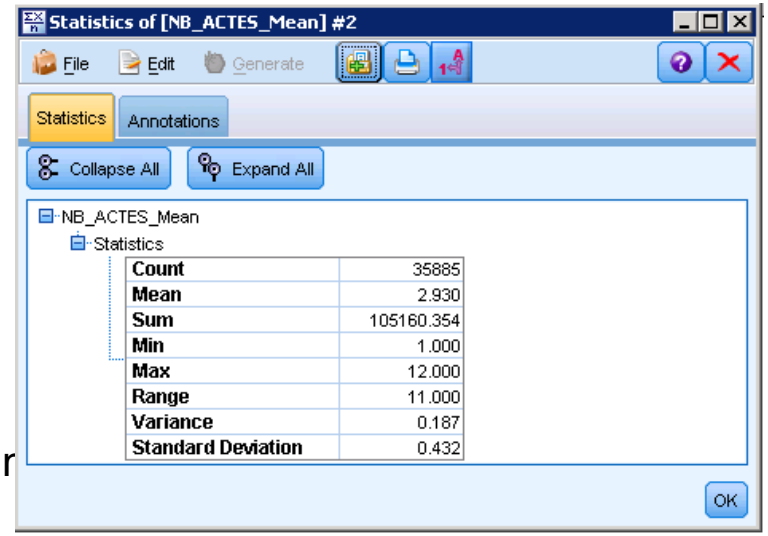
Methodology 1) Business Rules and Descriptive Analysis

Deviation modeling

The objective is to highlight potential alerts of fraud, thanks to business rules and statistics

- 8 Business Rules for Optic and 3 for Dental, following different analysis axis as the client
- 22 statistical indicators, following different analysis axis as the client





- (3,794= r

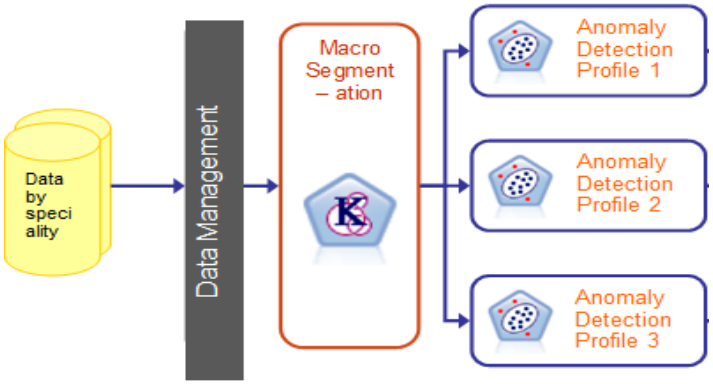
)00 Beneficiaries (500 Practitioners concerned)

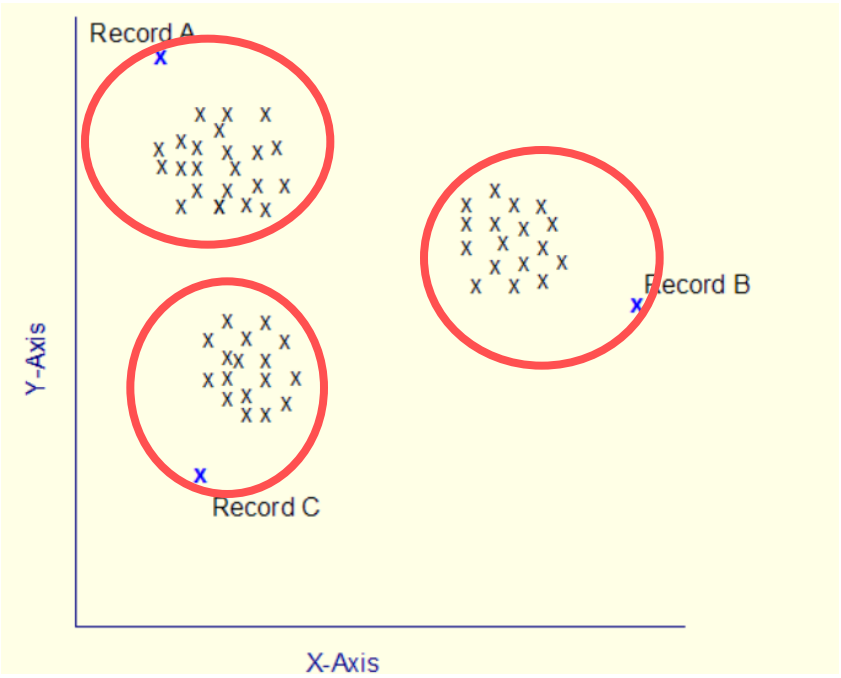
  - Rule + Statistics: Alerts on 50 Beneficiaries (234 Practitioners concerned)

Methodology 2) Anomaly Detection methodology

The objective is to highlight anomalies, and so potential fraud, thanks to the « anomaly detection » mathematical technique

- Anomaly detection is the search for items or events which do not conform to an expected pattern.
- Anomaly detection is an non supervised method: it does not require a training dataset containing known cases of fraud to use as a starting point





Methodology 3) FAMS methodology

The objective is to profile Practitioners, then to determine the risk of fraud, thanks to insights and statistics

- This methodology is based on an IBM asset/solution, named « Fraud and Abuse Management System».

- It is based on business rules and Practitioners attributes and statistics (like the total of visits) from the Healthcare industry:
  - Identification of abnormal behaviors for a given speciality and location
  - Built with more of 7000 indicators from 40 implemented projects (public sector and private customers)

Fraud Risk Scoring

IBM Fraud and Abuse Management System

Visualization Report Card

ID : 132650649
Name : (N/A)

Peer Group : OPTICAL — Optical
Model : OPTICS — Optics Model
Profile : 002 — All Optical Providers

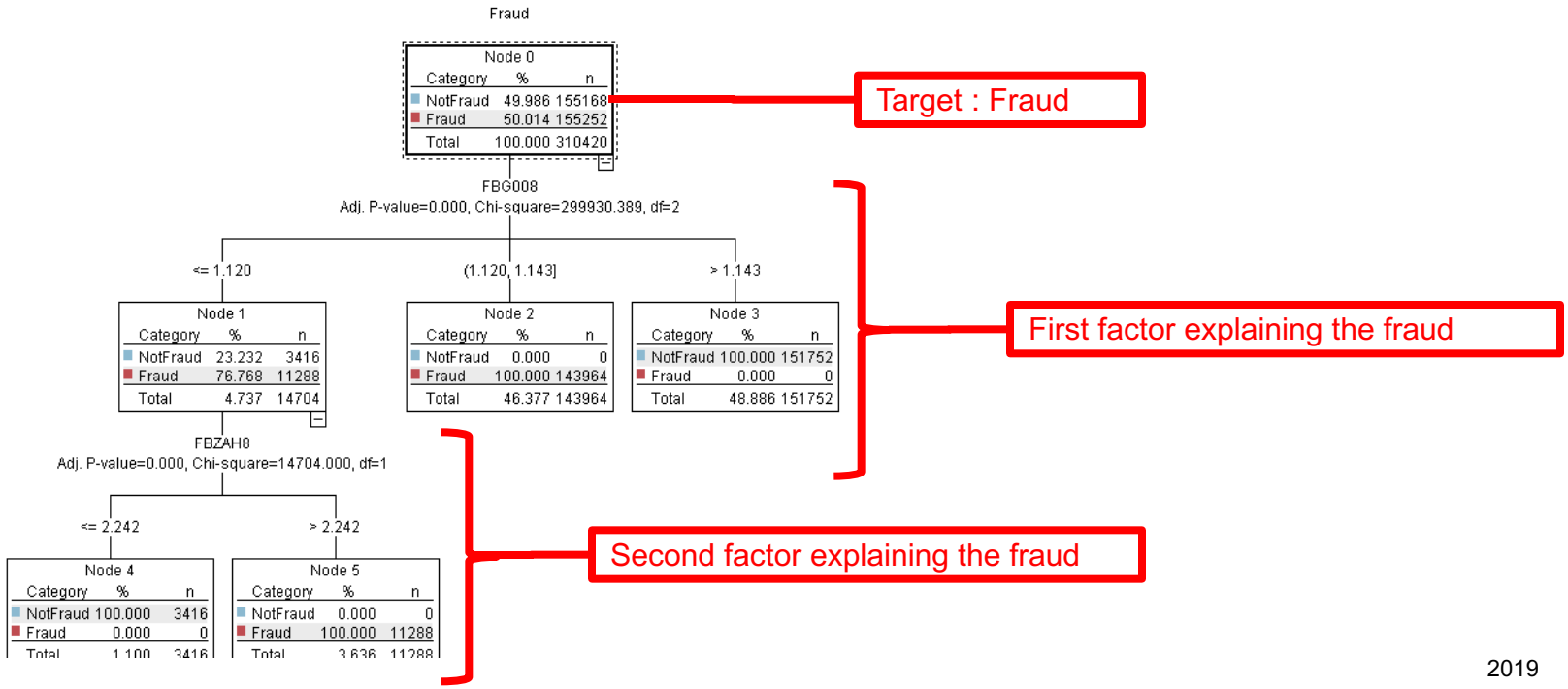
Element	Description	Rank	Score	Value	Minimum	Median	Maximum	Weight
COMPOSITE	**Provider Composite Score**	1	850	0.00	0.00	179.89	850.55	0.00
INFORMATION								
SIG_FEAT	Number of Significant Features	0	0	21.00	5.00	15.00	27.00	0.00
FBG010	Avg Age of Patients	10057	8	51.00	1.00	47.63	100.00	1.00
SPEC	Specialty Code		54					
CHRG	**Charges Group**	1	1000		0.00	12.55	1,000.00	1.00
FBG002	Avg € Charged/Patient	1	1000	8,360.00	7.00	694.57	2,120.00	1.00
FBG004	Avg € Charged/Visit	7	1000	2,786.67	7.00	658.50	1,920.00	1.00
FBG005	Avg € Charged/Px	92	1000	348.33	4.00	145.28	380.00	1.00
EXPOSURE	**Exposure**	3422	1		0.91	1.00	722.22	0.00
FBG003	Total € Charged	3329	1	8,360.00	7.00	3,988.00	564,071.00	1.00
FBG007	Total # of Visits	8623	1	3.00	1.00	6.00	661.00	1.00
FBG019	Total # of Patients	10957	1	1.00	1.00	6.00	587.00	1.00
FBG020	Total # of Procedures	6872	1	24.00	1.00	28.00	3,590.00	1.00
FBG334	Total # of Claims	8684	1	4.00	1.00	6.00	631.00	1.00
FBG449	Total € Paid	3409	1	3,200.00	0.00	1,524.00	243,921.00	1.00
LUN	**LUN**	44	801		0.00	244.29	1,000.00	1.00
FBZAF8	Avg # of Monture > 18 / Patient	1	1000	8.00	0.00	1.87	4.17	1.00
FBZAFH	Avg $ Paid in Monture > 18/ Patient	2	1000	800.00	0.00	115.07	383.80	1.00
FBZAG8	Avg # of Monture < 18/ Patient	6697	0	0.00	0.00	0.00	4.00	1.00
FBZAGH	Avg $ Paid in Monture < 18 / Patient	10268	0	0.00	0.00	0.00	246.50	1.00
FBZAH8	Avg # of LUN / Patient	1	1000	8.00	0.00	1.88	4.00	1.00
FBZAHH	Avg € Paid in LUN / Patient	2	1000	800.00	0.00	112.15	360.00	1.00
PAY	**Payments Group**	57	999		0.00	7.93	1,000.00	1.00
FBG636	Avg € Paid/Patient	1	1000	3,200.00	0.00	263.33	901.00	1.00
FBG637	Avg € Paid/Visit	9	1000	1,066.67	0.00	252.00	817.00	1.00
FBG638	Avg € Paid/Procedure	242	999	133.33	0.00	54.83	175.46	1.00
UPC	**Upcoding**	604	0		0.00	0.00	1,000.00	1.00

12/06/2013 10:32:44 Page 1

Methodology 4) Predictive Fraud patterns

The objective is to detect fraudulent new requests of reimbursment, thanks to predictive fraud patterns

- This methodology is based on known fradulent cases and creates predictive patterns or models able to identify criteria or variables explaining the fraud
- Predictive patterns are applied on new requests of reimbursment
- This methodology is supervized, that means it is based on historical known fraudulent cases. It uses classification predictive models (decision tree, neural networks, …).



Thank You

Yann Gouedo
Data Scientist Leader – Machine Learning / Artificial Intelligence
Marketing / Risk / Fraud / Maintenance
IBM Certified Senior Data Scientist & IBM Certified Senior Architect