2.3. Fraud Detection Techniques #Detection

2.3.1 Intro

Fraud-detection approaches have evolved and gained significant power over the past years.

- Adopting powerful *statistically-based methodologies*.
- Analyzing *massive amounts of data*.

Frauds remain a dynamic phenomenon hard to detect

1. **Fraudsters *adapt*** their approaches to *commit fraud without being exposed.*
   Probe fraud-detection and prevention systems:
   - To *understand* their *functioning*.
   - To *discover* their *weaknesses*.
2. **Fraudsters *develop*** advanced strategies to **cover/blend in** their tracks to **avoid being detected** ~ *camouflage*

2.3.2 Fraud-Detection Techniques #Techniques

Need for *new techniques* that are able to **detect and address stealthy patterns.**

1. Unsupervised learning or *descriptive analytics* techniques.
2. Supervised learning or *predictive analytics* techniques.

2.3.2.1 Unsupervised learning techniques or descriptive analytics

Unsupervised: #Unsupervised

- They do **not** require *labeled observations*.
- Learn from historical observation:
  Behavior that deviates from normal one = **Detecting anomalies**.

Allow **detecting novel fraud pattern**, not discovered by expert systems since they:

- Are *different* in nature *from historical fraud*.
- Make *use* of *new, unknown mechanisms*.

In the end:

> ***Complementary tool*** *to improve its expert rule-based fraud-detection system*.

Limitations: #Limitations
Detect if a *new fraud mechanism* leads to *detectable deviations from normality*.
Prone to deception: *camouflage-like* fraud strategies.

> *Need to be improved by complementing other tools.*

2.3.2.2 Supervised learning techniques or predictive analytics

Supervised: #Supervised

#DEF **Learn from historical observations to retrieve patterns that allow differentiating normal and fraudulent behavior.**

Aim at *finding "known alarms"*: tracks that fraudsters *cannot* hide.

Can be applied to:

- **Predict fraud.**
- **Detect fraud.**
- **Estimate the amount of fraud.**

Limitations: #Limitations

1. They *need historical examples to learn* from (i.e., a labeled data set of historically observed fraud behavior).
2. *Low detection power against different and new fraud types* (i.e., not detected so far and not included in the historical database of fraud) -> detected by descriptive analytics.

Complementarity of supervised and unsupervised methods:
Use of *both methods* in developing a *powerful fraud-detection and prevention system*, they focus on *different aspects of fraud*.

2.3.2.3 Social network analysis

Extends the abilities of the fraud-detection system by *learning and detecting characteristics* of fraudulent behavior *in a network of linked entities*.
Including an extra source of information in the analysis, being the relationships between entities, it *contributes in uncovering particular patterns indicating fraud*.

2.3.3 Developing a fraud-detection system

1. **Expert-based rule engine**.
2. **Unsupervised learning systems**.
3. **Supervised learning systems**.

The exact order of adopting the different techniques depend on the characteristics of the type of fraud.

Next chapter: Fraud Management Cycle