2.2 Anti-Fraud Strategy #AntiFraud

2.2.1 Intro

This systems serve to hinder as much as possible fraudsters and other criminals.

- #DEF #FraudDetection **Fraud Detection**: we try to recognize or discover fraudulent activities (also called *ex-post approach*, after the fact has happened).
- #DEF #FraudPrevention **Fraud Prevention**: we try to entirely avoid or reduce fraud (also called *ex-ante approach*, before the fact has happend).

2.2.2 Fraud Prevention Examples #PreventionExamples

STRONG CUSTOMER AUTHENTICATION (PSD2)** #PSD2

PSD2 is a european regulatory requirement designed to:

- Reduce fraud;
- More secure online payments. #SCA
  Achieved by meeting **SCA** (**S**ecure **C**ustomer **A**uthentication) **requirements**, namely authentication must use at least two of these factors:
  - Something the customer *knows* (PIN, password ecc.);
  - Something the customer *has* (phone, tablet ecc.);
  - Something the customer *is* (fingerprint, face recognition ecc.).

This standard is now required in every online payment within Europe except for these cases:

- Low risk transactions;
- Payments below 30€;
- Fixed-amount subscription;
- Transactions initiated by the seller;
- Trusted beneficiaries;
- Phone sales;
- Corporate payments.

Ways to secure a payment:

- 3D Secure
- 3D Secure 2
- Apple Pay or Google Pay

ONE-TIME PASSWORD GENERATORS (OTP) #OTP

CIAO

SMART CARDS (OR USB KEYS) #SMARTCARDS

CIAO

2.2.3 Fraud Detection and Fraud Prevention #AntiFraudLifecycle

Anti-Fraud strategies cycle:

1. Fraud Detection or Prevention mechanism deployed;
2. Fraudsters adapt and change their behavior;
3. Decrease in fraud detection or prevention power;
4. Back to point 1.

From this facts, we can infer that an effective anti-fraud strategy has 4 main points:

1. Prevention;
2. Detection;
3. Deterrence;
4. Response.

2.2.4 Expert-based Approach #ExpertBasedApproach

#DEF Anti-Fraud approach built on the *domain knowledge* of the **fraud analyst**.

This approach is carried out by doing **manual investigations** of suspicious cases.

Whenever a new fraud scheme is found, a **detailed investigation** is requiered in order to address how to tackle the new threat.
==> Once the new fraud mechanism is comprehended, the fraud detection and prevention mechanisms are extended.

2.2.4.1 Rule-based engine #RuleBasedEngine

If-Then Rules: With a rule-based engine, previously detected fraud patterns are defined in rules that are then applied to transactions and trigger an alert when a fraud may be committed. #IfThenRules

Disadvantages:

- **Expensive** to deploy;
  - Requieres manual input;
  - Difficult to update and mantain
    ==> Every signaled case requires human follow-up and investigation.
- **Fraudsters** can **learn** the rules and **circumvent** them
- **New fraud** patterns are **not** automatically **signaled**

> *A rule-based engine must continuously monitored, improved,and updated to remain effective.*

Rule-based engine VS Automated Fraud-Detection Systems

- Expert-based fraud-detection system relies on human expert input, evaluation, and monitoring ==> labour intensive, requires human interventions.
- Automated Fraud-Detection Systems require less human involvement and could lead to a more efficient and effective system.

However, expert knowledge remains crucial in order to build effective systems.

2.2.5 Fraud Management #FraudManagement

Upon detection of a fraudolent activity, two measures can be taken:

- Corrective measures;
- Preventive measures.

2.2.5.1 Corrective Measures

Corrective measures aim to **resolve** the fraud and **correct** the consequences.

With this approach, actions are taken to **retrospectively detect** and subsequently **address** similar **fraud cases**.
This retrospective approach is composed of two phases:

- Assessment of the impact of the newly detected type of fraud;
- Resolution, by means of corrective measures.

The **sooner** the **corrective measures** are **taken** and fraud is detected ==> the **more effective** such **measures are** and the more **losses** can be **avoided**.

2.2.5.2 Preventive Measures

Actions that aim at **preventing future frauds**, making the **organization** more robust and **less vulnerable**.

Usual process:

1. **Investigate** the fraud case to understand the underlying mechanisms.
2. **Extend** the available expert **knowledge** with the discovered mechanisms.
3. **Adjust** the detection and prevention system.

2.2.5.3 Fraud Becomes Easier to Detect As Time Passes

Cycle:

1. A **new fraud** mechasism is **used**;
2. **Increase** in the usage:
    - Fraudsters share the knowledge about this new type of fraud.
3. Fraud becomes **more popular** and **statistically easier** to **detect**;
4. **Fraudsters' risk** of being exposed **increases**;
5. The **fraud** mechanism is **discovered** and **detected**;
6. Similar **frauds**, committed **in the past**, are **discovered**.

> *The **more frauds** are **discovered** ==> the **more data** is collected and is **available** ==> **Better** detection **techniques** are being **developed***

2.2.6 Data-Driven Fraud Detection

Data-driven fraud detection in an **approach** that shifts the **focus** of the technique from the expertise of the expert to the **data collected** on previous **frauds**.
Classic expert-based fraud-detection approaches are:

- **Widespread**;
- The **starting point** for anti-fraud strategies and a **complementary tool** to data-driven fraud detection.

⚠ **Problem**: Organizations have a limited investigation capacity.

A **shift** is taking place **toward data-driven** or **statistically-based** fraud-detection systems, in order to optimize:

- Precision
- Operational efficiency
- Cost efficiency

2.2.6.1 Precision

Data-driven fraud detection **increases detection power** w.r.t to classic approaches. This is because it **processess massive volumes** of **information to uncover frauds** that are not apparent to the human eye.

🎯 Massive volumes of information ==> Higher precision in detection

> *Higher precision ==> Higher fraction of frauds inspected*

2.2.6.2 Operational and Cost Efficiency

Increasing amount of cases to be analyzed ==> requires automated processes.

Operational requirements exist ==> imposing time constraints on the processing of a case.

Next Chapter: Fraud Detection Techniques