FRAUD MANAGEMENT.
HOW TO DETECT FRAUDS AND ACT AGAINST THEM BEFORE THEY OCCUR

Focusing both on processes and systems, Reply provides innovative solutions for Fraud Management based on Business Rules Management Systems (BRMS). With a BRMS-based approach, organizations can analyze their own data in order to prevent and fight against fraud, ensuring the business profitability. Through in-depth knowledge of Telco&Media processes combined with system design competence, Reply helps organizations to achieve a faster return on investment.

FRAUD

Fraud is an intentional deception made for personal gain in order to obtain unauthorized benefits (money, property, etc.); examples of frauds are the use of services without paying the due amount, the appropriation of money through the improper use of means of payment, etc.

The continuous market and technology developments provide people intending to commit fraud with new scenarios and new methods to carry out fraudulent practices. The Fraud Management System supports the businesses affected by these events (such as Banks, Media and Telco), provides them with the tools required for the assessment, control and even prevention of these practices in order to limit and avoid money and image loss and leveraging the wealth of information provided.

Fraud is an intentional deception made for personal gain in order to obtain unauthorized benefits (money, property, etc.); Fraud can be carried out in legal, commercial, tax, monetary scenarios as well as in sports, food and bank industries.
IDENTITY THEFT

Quick and continuous market changes and technology developments provide people intending to commit Fraud with new scenarios and methods. This is a consequence of the increasing use of Information Technology tools (Internet and PC) which do not require people to reveal the identity or to be physically present in order to be identified. The new Information Technology tools can be used provided users have valid credentials; if, however, these credentials are not adequately protected, they can be stolen and used by other users.

A survey on 50 different countries considering 4000 companies has shown that the number of companies which have become victims of fraud in Western Europe has increased by 5% from 2001 to 2003 reaching 34% in 2005, while this number has increased by 11% reaching 37% in Central and Eastern Europe.

Italy is severely damaged by fraud and from recent studies (carried out in 2004) it results that Italy - unfortunately - holds the second place in Europe after Great Britain, as for fraud practices committed using false or stolen credentials. Identity Fraud is commonly known as "Identity Theft".

IMAGE LOSS

The substantial increase of online credit card transactions or online bank transactions has resulted in a huge increase of fraudulent practices. In the Telco & Media Market, the value of losses due to Identity Theft is often identified with the value of physical or hardware devices, but image losses are often greater.

ADVANTAGES RESULTING FROM THE ADOPTION OF A FRAUD PREVENTION SOLUTION

As far as the adoption of an Anti-Fraud Solution is concerned, critical success factors can be identified in the steps envisaging the creation and the offer of services to customers. As for the management of frauds, it is also very important to focus on processes, laws and regulations (Basel II).

Economic advantages resulting from the adoption of a fraud management solution are linked to the economic loss reduction associated with the use of services by customers not entitled to or related to either identity theft or, in general, to illegal practices.
Although not directly linked to loss reduction, other advantages result from the adoption of a fraud management solution:

- Greater value of the services provided to customers as the adoption of certified Anti-Fraud systems guarantees high security,
- Decrease and control of new subscriptions/acquisitions with ascertained Fraud practices,
- Costs cutting linked to Credit recovery in fraudulent practices
- Decrease in the number of reports for non-identified transactions: Customer Retention and Win Back
- Competitive edge through a better and faster fraud management that consequently results in an opportunity to increase revenues
- “Fraud shift” towards competitors

**PROCESS SYNERGY**

The ideal approach shall involve the whole company and its processes in order to provide the key solution defining the Fraud Management Solution.

The functional model for the definition of an anti-fraud solution is based on three different components:
• **Prevention**: It includes all the components of the key value such as the customer identity, the creation and delivery of the service, new IT applications and technologies, new operations and business processes, adequate SLAs
• **Detection and management**: It includes decision-making and back-office processes
• **Analysis and investigation**: It includes KPIs and data analyses

In general, the first solution adopted is Data Mining. The analysis to be carried out on company data will for sure be time-intensive and complex and require a serious computational ability in order to identify appropriate statistical models for the definition of the prevention rules based on data analysis. A data mining technology enables to collect, analyze and prevent different fraudulent practices. Data mining techniques are based on the analysis and investigation of a huge database in order to define models and rules.

**BUSINESS RULES: THE “AGILE” MODEL**

**BUSINESS RULE**

A Business Rule is a rule implementing or changing the behavior of a business application in accordance with the factors interacting with it. The rule defines the logic that must be applied by all the software components which are part of a business application.

The critical success factor of a company which must react to changes is the immediate, prompt and flexible use of each new business rule. BRMSs support the business requirements for continuous changes without requiring the re-engineering of IT applications.

A Fraud Management infrastructure supported by a BRMS (Business Rules Management System) can effectively and efficiently meet Fraud management strategies by increasing the flexibility and the adaptability of the different types of adopted solutions through:

- an easy definition of new rules
- a quick removal of the existing rules
- tool boxes which can be used with simple boolean operators
- the powerful use of “natural language” for the definition of the rules
- the use of a powerful deductive method
- the possibility to immediately assess the performances of new rules without a dual system
- the opportunity to enter in the rule flow new cases based on the rules to “be tested”
Main Fraud Management Processes

- **Data entry**: even from different and heterogeneous sources
- **Data standardization and analysis** (Alias matching, Data Integrity Check) based on Business Rules (BRMS)
- **Management of evidence and facts**: through a dynamic and configurable model based on Business Rules (BRMS) – Data Mining techniques
- **Case generation and risk assessment**: through a workflow (a BPM if complexity is increasing) modelled by a deductive BRMS
- **Case management and reporting**: through a workflow (a BPM if complexity is increasing) modelled by a deductive BRMS

**FRAUD PREVENTION SOLUTION: ARCHITECTURE MODEL**

As opposed to the traditional solutions with a single approach, BRMS-based solutions analyze company data through business rules; another advantage offered by these solutions is that the applications built with BRMS are able to transmit data with flexibility and promptness improving therefore the whole infrastructure policy of the company.
The business rules are expressions resulting from policies, rules and procedures which are included in the system (ILOG source, Inc.). The Functional architecture of the figure is based on the Ilog BRMS.

Sytel Reply is the company of the Reply Group specialized in the Telco Market. Sytel Reply’s mission is to support telecommunications operators in the technology and application innovation by designing, deploying and managing systems addressed to the BSS and OSS areas.

Leveraging its expertise and competence, Sytel Reply deploys a team of professionals able to support customers in each phase of the project: system design, requirements analysis, software development and go-live.

Sytel Reply
www.reply.eu