



IT & Operating Model

HOW TO DERIVE VALUE FROM “ARTIFICIAL ADAPTIVE SYSTEMS”

The fraudulent behaviors in the Telecommunications market are traditionally very complex to a point where they look turbulent in their continuous development and extremely high variability, which is due to the rapid technological evolution. All of this requires the Telecom companies to invest substantially in anti-fraud research and innovation processes, as well as to suffer high running costs for the maintenance of appropriate security standards.

The usual technologies which are currently utilized to address and prevent credit and fraud risks have significant limitations both in relation to costs and their vulnerability. For this reason, Be has developed new innovative technologies based on quantitative methods, which are able to continuously learn from the observed behavior and, consequently, to rapidly adapt to the evolution of the “attack patterns” . In addition, the variety of Be services also includes best-of-breed technologies which allow our clients to innovate their internal processes at a very competitive cost.

This month Be is finalizing a first pilot of “Artificial Adaptive Systems” for one of the leading Italian Telecom operators, which will lead to a second experimental project for next 6 months. The tactical goal of this project is to automate part of the manual work, based on the experience of experts in assessing the consistency of the information provided at the time of underwriting a new customer. The strategic goal is to fully exploit the potential of our tools in the preliminary assessment of “client risk”,



HOW TO DERIVE VALUE FROM "ARTIFICIAL ADAPTIVE SYSTEMS"

through a joint analysis of company data available from CRM and other systems, and information provided by the client himself in the underwriting phase.

The use of our technologies is meant to support analysts in developing highly specialized professional skills in anti-fraud detection, as it will allow them to focus on the most critical and valuable fraud instances. This will result in both an anti-fraud performance improvement (in terms of effectiveness of results) and a significant saving coming from more efficient organizational processes.