The Adaptive Classification Engine is an optional component of Fractals which provides automated, intelligent fraud detection by using a combination of Bayesian statistical analysis and proprietary inference techniques from NCR.

Staying ahead of global fraud is a never-ending battle. As the market for electronic payments becomes bigger and more diverse so do the chances of a damaging fraud attack.

Around the world, issuers, acquirers, merchants, processors and PSPs rely on Fractals for intelligent fraud detection and prevention. Its distinctive combination of user-defined rules and self-learning analytical models provide both exceptionally high levels of fraud detection and low rates of false positives.

Every day, businesses of all sizes protect their customers, their reputation and their bottom line from fraud using Fractals from NCR.

For more information, visit us at ncr.com.
The Fractals Adaptive Classification Engine

The Adaptive Classification Engine is an optional component of Fractals which provides automated, intelligent fraud detection by using a combination of Bayesian statistical analysis and proprietary inference techniques from NCR. By applying mathematical models to each incoming transaction it identifies suspicious activity, calculates a probability-based fraud score that indicates the likelihood of fraud, and then triggers an action.

The model is initially set and tuned using your own recent historical data and fraud tags so that it can identify the unique fraud patterns facing your organization. If you have analytical specialists in-house, you can also input your own fraud-scoring models into the Adaptive Classification Engine.

The result is a bespoke and highly accurate fraud detection model that can be set up in just a few short weeks – giving you the best performance right from the start.

Each model in the Adaptive Classification Engine is based on a series of mathematical algorithms that are targeted at identifying specific fraud patterns or irregularities in account holder behavior. Fractals can execute numerous algorithms simultaneously. A customer’s model typically contains between 20 and 45 separate algorithms and individual models can be established for certain account types or customer segments for even greater granularity. The Adaptive Classification Engine model includes strategies that can learn rapidly as frauds are tagged in the system. Once in production, it carries on learning and self-calibrating. Not only does this ensure that Fractals can track and react rapidly to changing fraud trends, it frees your fraud analysts to focus on more value-added tasks.

One of the key benefits of our Adaptive Classification Engine compared with traditional Neural Network models is the transparency with which we can deliver our results to the end user.

Unlike a Neural Network which is a black box, our scores are delivered with a clear set of reasons and probabilities related to each transaction score. This “white box” approach gives the end user much more granular information to work from when assessing a transaction or speaking with a customer, and more information means better customer service: the key to successful fraud operations.
Accurate analysis for all businesses

The initial mathematical model for your organization is quick to build. After that, model maintenance is both rapid and cost-effective. Organizations that deploy the Fractals Adaptive Classification Engine typically see impressive results from the very first transaction and high detection rates remain consistent over several years. At the same time, false positive rates remain exceptionally low.

For example, an organization achieved a fraud detection rate of 80 percent before any user-specified rules were implemented and 65 percent of highlighted frauds were detected on the first transaction.

The Adaptive Classification Engine also uses the initial training data set very efficiently, so it can calibrate its models using relatively small data sets. As a result, it can produce customized, cost-effective and accurate detection models for organizations with small or medium-sized customer portfolios, in addition to the largest institutions.

The Adaptive Classification Engine also enables you to adjust the threshold levels for fraud detection to match the alert-handling capacity of your fraud analysts.

The Fractals Rules Engine

The Adaptive Classification Engine is normally deployed together with the Fractals Rules Engine, which enables you to define the rules used to score each transaction and determine whether it should be authorized, declined or reviewed.

You access the rules engine through a browser-based interface and define, create, test, evaluate and deploy rules without coding or programming. Fractals’ graphical rule workbench also makes it easy to express complex and varied rules, and update them rapidly in response to changing threats.

The Adaptive Classification Engine can also be implemented to supplement poorly performing scoring or rules engines.
Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries. The company encourages investors to visit its web site which is updated regularly with financial and other important information about NCR.

The Adaptive Classification Engine at a glance

- Detects extremely high numbers of fraud cases independently of fraud analysts and rules engines.
- Scores and reviews fraud scores in real time enabling in-flight fraud blocking.
- Creates and calibrates individual strategies for specific card or account types.
- Adjusts false-positive threshold to suit the case handling capacity of your fraud analysts.
- Frees analysts to focus on value-added tasks such as strategy development, trend analysis and business intelligence.
- White box approach delivers maximum information for analysts to work with when investigating a case.
- Makes use of targeted, customized detection models based on your own fraud patterns.
- Can incorporate your own fraud-scoring models for bespoke fraud detection.
- Continuously learns and self-calibrates for greater accuracy and effectiveness at low cost.
- Delivers excellent results for both large and small customer bases.
- Clearly shows the user causes of individual fraud scores for greater insight into fraudulent activity.
- Is certified as a PA-DSS compliant solution.