

# FRACTALS

## Acquirer Fraud Detection – MRA and Acquirer Rules

**An integral component of the Fractals Framework, the Rules Engine offers a powerful rule capability aimed at acquirer fraud detection and based on two types of rule, MRA Rules and Acquirer Rules, which enable an institution to readily meet and exceed Visa stipulated minimum requirements for merchant risk monitoring.**

**Rules Engine**

Fractals Rules Engine enables client staff to deploy fraud detection rules which they have conceived empirically, based on their observation and knowledge of fraud patterns.

The Rules Engine complements the sophisticated probabilistic alerting provided by ACE, the Adaptive Classification Engine, allowing client staff to respond immediately to a sudden fraud attack, to knowledge of potential future fraud attacks obtained from market sources or to identify and intercept known fraud patterns.

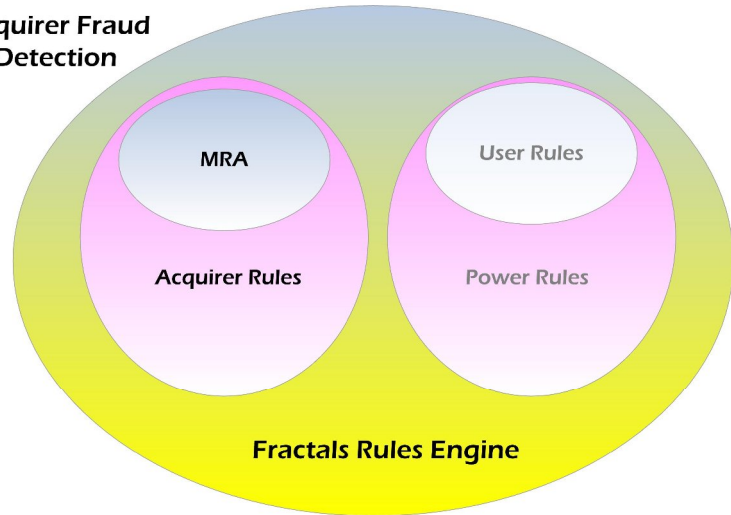
Fractals can be deployed in a Rules Engine-only configuration, enabling organizations to take advantage of its powerful rule construction, management and deployment facilities, or together with ACE to provide an all encompassing fraud detection/prevention framework.

*Third party integration*

Fractals can be deployed together with Alaric’s Authentic authorization and acquiring product.

However, Fractals can be used in conjunction with third party authorization systems as well. In such a scenario, Alaric’s well

Acquirer Fraud Detection



honed skills and expertise in payments integration come to the fore to enable rapid, cost effective integration with the client’s authorization system.

Alaric’s Message Mapper and Authentic Gateway products are particularly relevant to achieving such third party integration and their deployment can dramatically shorten integration time and cost, which is usually a major cost factor when deploying other fraud detection solutions.

*User oriented*

The system is designed to be used by fraud analysts rather than IT technicians. Detection rules are created using familiar Windows-based point and click technology, which requires no programming or database knowledge.

**Acquirer fraud detection**

Using Fractals MRA and Acquirer Rules, acquirers can protect themselves from costly fraud attacks, including:

- merchant default (where a merchant defaults on its payments or disappears without settling its bills).
- fraudulent transactions acquired from specific

**Fast Facts**  
**MRA & Acquirer Rules**

- ✓ Point-&-click rule creation, user-defined acquirer detection rules, without coding
- ✓ Visa & PABP PCI DSS compliant
- ✓ Acquirer Rules for enhanced detection performance
- ✓ Real time, near real time and batch operation
- ✓ Rule evaluation & duplicate checking capability
- ✓ Browser based, ideal for distributed operation
- ✓ 100% Java, runs on UNIX, Linux & Windows

merchants, indicative of a fraudulent merchant or fraudulent merchant staff.

- fraudulent transactions acquired from third party bank cards.
- fraudulent transactions acquired via international cards used in the domestic market.

*Visa compliant*

Banks issuing Visa cards and acquiring Visa cards and



acquiring Visa transactions are mandated to implement fraud detection systems that meet Visa's minimum requirements for both issuer and acquirer fraud monitoring.

### Acquirer Rule types

Fractals provides two classes of rule for acquirer fraud detection, namely, *MRA Rules* (=Merchant Ratio Analysis Rules) and *Acquirer Rules*.

Fractals MRA Rules are executed periodically, in batch mode, and enable an organization to satisfy Visa's minimum requirements for acquirer fraud monitoring and enable mandate compliance using a standard product solution.

Acquirer Rules enable an altogether higher level of fraud detection performance to be achieved, generalizing MRA Rules for real time use.

### MRA Rules

MRA operates in batch mode and processes authorization and settlement data via a series of rules relating to merchant activity. These rules are as specified by Visa. MRA provides a flexible implementation of these rules via an easy-to-use browser-based interface.

### How MRA works

Each of the MRA Rules operates by comparing the activity of a merchant against certain pre-defined thresholds. Fractals offers a flexible, sophisticated implementation in that default thresholds can be individually set for groups of merchants, account numbers or BINs, for groups of merchants, card numbers and BINs.

If the merchant activity for a given day exceeds the calculated threshold for any of the rules, an alert is raised for that merchant and an alert trigger is raised for each of the

rules that have been broken by the merchant.

### Merchant Alert List

The Merchant Alert List screen allows the user to display merchant alerts using a number of filters and allows alerts to be assigned to a selected user.

Alerts can be sorted in a variety of orders e.g. by merchant alert date, merchant alert type, rules broken etc. Rules triggered for the selected alert are displayed, as well as the change history for the selected alert and the merchant details.

### Merchant Group Maintenance

Fractals allows merchants with similar characteristics to be grouped. This means thresholds can be set at the group level, rather than merchant by merchant, the latter being time consuming and error prone. The Merchant Group Maintenance screen allows the user to create and update groups of merchants.

In this way, merchants can be set up with default group thresholds which can be overridden with specific thresholds for specific merchants, if desired.

### Merchant Rules Maintenance

Fractals MRA comes with the merchant rule records pre-populated in the database, with an entry relating to each of the MRA rules that are run to produce the merchant alerts. These rule records contain a threshold value which relates to the rule which can be overridden for a group of merchants or for an individual merchant.

### Acquirer Rules

Acquirer Rules are the counterpart of Fractals' Issuer User Rules with Power Components and share the same underlying technology.

Fractals makes available to Acquirer Rules, *inter alia*, all the derived variables which underpin the Visa-specified MRA Rules. Using the Rules Administration Workbench, analysts can construct Acquirer Rules of arbitrary complexity which act on the latter derived variables. Acquirer Rules operate in near real time or real time according to client preference. In the latter case, alerts from Acquirer Rules can be fed back to the card acquiring system to influence the processing of a given transaction, in real time.

### Fast deployment at low cost

Implementation of acquirer fraud detection rules in other systems is often a programming or scripting task which needs to be performed by the product vendor or by the client's own IT staff, involving the client in time delay and high cost.

In contrast, Fractals' MRA and Acquirer Rules are configurable by non-IT staff and so are under the fraud department's direct control - rules can be conceived, tested and deployed into the live environment in a matter of minutes.

This enables the institution to react instantly to any specific intelligence it has gleaned from market sources or card associations, all at zero incremental cost.

### Technology platform

Written in Java, the Fractals Rules Engine is platform independent.

The heart of the Rules Engine is its user interface, the Rules Administration Workbench, or RAW, which is Windows browser-based and is well suited to distributed operation.

