

# FRACTALS

## Issuer Fraud Detection - User Rules

*An integral component of the Fractals Framework, the Rules Engine generates fraud alerts by applying user-defined rules to incoming transaction flows. The Rules Engine is applicable to both issuer and acquirer fraud detection. This fact sheet outlines the Rule Engine's issuer fraud detection capability.*

### 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.

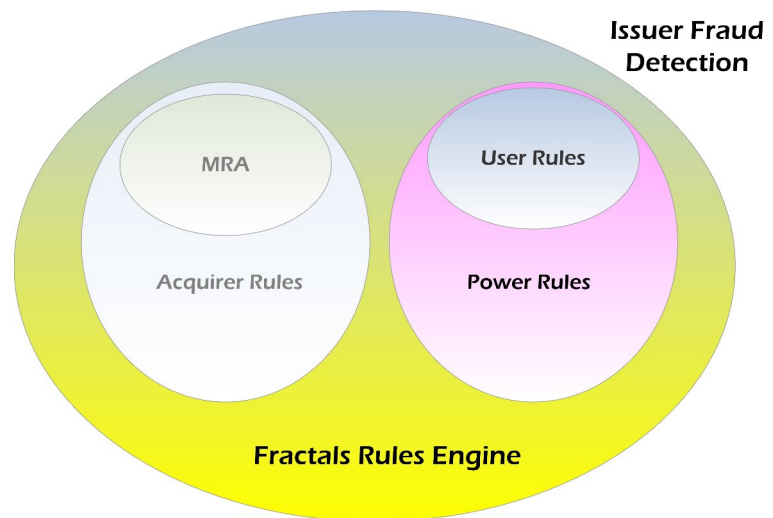
The Rules Engine complements the sophisticated probabilistic alerting provided by ACE, the Adaptive Classification Engine, allowing client staff to respond immediately to a sudden fraud attack, to knowledge of potential future fraud attacks obtained from market sources and to identify and intercept known 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 may be deployed together with Alaric's Authentic authorization/acquiring product.

However, Fractals can also be used in conjunction with third party authorization systems as well. In such a scenario, Alaric's well 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 Authentic Gateway product is particularly relevant to achieving such third party integration and its 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.

### Powerful User Rules

User Rules are potent transaction fraud detectors in their own right. For example, User Rules:

- can be executed against any type of transaction
- can operate on any data items present in a transaction or sequence of transactions
- can operate on highly predictive variables derived

### Fast Facts Issuer Rules

- ✓ Point-&-click rule creation, user-defined detection rules, without coding
- ✓ Power Rules for enhanced detection performance
- ✓ Real time, near real time and batch operation
- ✓ Rule evaluation & duplicate checking capability
- ✓ Browser based, ideal for distributed operation
- ✓ Single or multi-banking operation
- ✓ 100% Java, supports UNIX, Linux and Windows operating systems

from sequences of transactions (e.g. rolling averages, rolling counts, velocities etc)

- can operate in batch, near real-time or real-time modes of operation
- can be applied to identify sequential and rapid spend fraud patterns (i.e. patterns that exist in transactions that run directly one after the other)



- can be applied across a time base to detect counterfeit and lost and stolen type fraud patterns where fraudulent transactions appear on an account some time after the point at which the card was first compromised.

In summary, User Rules offer an easy-to-manage transaction monitoring capability for both fraud and risk.

#### *Configuring rules*

Rules are configured using the browser-based Rule Administration Workbench (RAW).

Rules are built up component by component via the intuitive RAW GUI, which requires no programming or database knowledge. Copying and then modifying previously created rules is possible, enabling rapid development of new User Rules.

Fractals has useful constructs for use in rule components which enable what might otherwise be lengthy or multiple rules (e.g. those which involve checking against a card or merchant hot list) to be expressed in a very compact, intelligible and easily maintained form.

#### *Evaluating & monitoring rules*

Before deploying a new User Rule it is vital to know its likely alert generation rate - a rule is not of much use if it floods the fraud analyst with alerts.

The Rules Engine has an easy to use feature which forecasts the likely alert generation rate,

enabling the rule's creator to decide whether or not to deploy it.

Moreover, the Rules Engine continuously reports on User Rule detection performance enabling ineffective rules to be pruned or modified.

#### *Duplicates*

The Rules Engine also automatically checks that a User Rule does not duplicate a previously configured rule, thereby saving processing time and minimizing alerts generated.

#### *Activation and scheduling*

User Rules can be activated and deactivated at any time via the RAW. Additionally, there is a sophisticated rule scheduling capability, enabling rules to be activated at specified times of the day, on specific days of the week. This enables alert generation to be appropriately paced to match fraud analyst staffing levels.

#### **Fast deployment at low cost**

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

In contrast, Fractals' User Rules are configurable by non-IT staff and so can be 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.

#### **Operating modes**

Fractals' Rules Engine can be deployed in a multi-institution mode which, together with its browser-based, remotely accessible RAW, makes it ideally suited to processors and service providers.

The Rules Engine can also operate in multi-product mode for an institution with multiple card products, enabling detection rules to be deployed specific to each particular product.

#### **Online Real-Time**

The Rules Engine is designed for both fraud detection and fraud prevention modes of operation. In fraud prevention mode, the system enables the business to write rules that detect fraud in real-time and send refer or decline advice to the authorization system in real time, to enable fraud to be intercepted in flight, at authorization time.

