PRODUCT FACT SHEET

FRACTALS

Adaptive Solutions to Hi-tech Financial Crime

Fractals is a class leading integrated, intelligent fraud detection and prevention framework for issuers and acquirers of debit, credit and other types of payment cards.

Introducing Fractals

Fractals (Fraud Risk Analysis - Creation Testing and Learning System) is an integrated software framework for card fraud detection.

Fractals enables empirical knowledge and experience of fraud analysts to be combined with intelligent strategies automatically calibrated using Alaric's proprietary inference techniques based on Bayesian methods.

Fractals can operate in real time, near-real time and batch detection modes and provides a unified, comprehensive and effective solution to both issuer and acquirer fraud detection.

Ease of integration

Fraud alerts may be processed by fraud analysts or automatically fed back to a card authorization or acquiring system in real time. The latter necessitates tight, real time integration with the relevant system.

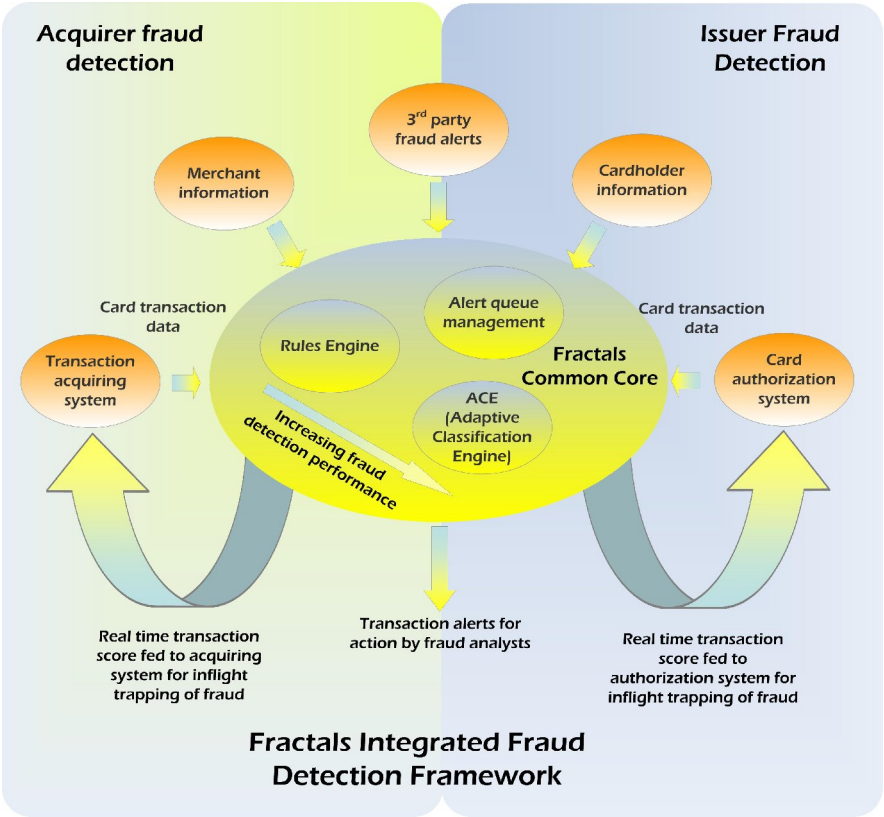
Alaric has the products and skills to effect such complex payments integration rapidly and cost effectively. In contrast, the integration cost of competitive fraud solutions may equal or exceed the cost of the fraud solutions themselves.

SOA orientation

Fractals is well suited to an SOA environment. Its functionality can be delivered as a Web Service via Alaric's Authentic Gateway.

Rules Engine

Fractals' Rules Engine enables incoming transactions to be alerted and scored via user defined detection rules from both issuer and acquirer perspectives.



Rules can be quickly created, tested and deployed using Fractals' browser-based GUI called the Rules Administration Workbench. No programming or database knowledge is required.

The Rules Engine provides a number of rule constructs as standard which make it possible to express complex and profuse rules in a very compact, intelligible form, which greatly facilitates rule maintenance and modfication.

The Rules Engine offers these types of rules:

User Rules

Oriented towards issuer fraud detection, so-called User Rules can be defined which act on data which is directly observable in a card transaction (for example, amount, country code) and also on derived variables, computed from a sequence of transactions.

MRA Rules

Merchant Ratio Analysis Rules are a core set of fraud detection rules for acquirers which are mandated as minimum requirements by Visa CEMEA but which are of general applicability.

Acquirer Rules

Acquirer Rules are based on derived variables which are directly indicative of acquirer fraud.

Adaptive Classification Engine

ACE is a major component of Fractals which operates separately from, but simultaneously with, the Rules Engine.

ACE provides intelligent fraud detection and generates fraud alerts by executing mathematical models against incoming transactions to

compute a fraud score or "probability of fraud".

Deployment

ACE is normally deployed together with the Rules Engine to provide a powerful, all encompassing fraud detection/prevention platform. However, customers requiring a purely automated detection system, without a rules capability, can deploy ACE standalone.

Model training

The ACE mathematical model is calibrated (or trained) using a dataset that contains a customer's historical transactions to enable ACE to recognize the fraud patterns present in this data. In order to do this, the customer provides several months of recent transaction data, with frauds tagged.

The parameters in the ACE detection algorithms then automatically adjust to identify the fraud patterns specific to this data and to produce a highly accurate fraud detection model.

The mathematical approach adopted in ACE means that model training is a very quick and finite process, making it economic to retrain the ACE model frequently, thereby ensuring that detection performance is continuously optimal.

Auto optimization

A significant direct consequence of the mathematical approach adopted in ACE is that it enables detection strategies to self optimize and detect new fraud patterns between model retrains, enabling a much higher detection rate to be maintained than is possible with a neural network, the detection performance of which tends to drop off a few months after a new model is deployed.

ACE provides high levels of fraud detection with low false positive ratios, representing a substantial improvement over the more traditional approaches using expert rules and neural networks.

Intelligibility

All alerts are based on probabilistic mathematical techniques, providing clear, auditable results, and can use external data sources (e.g. card scheme alerts) in the prioritization process.

Alert queue management

Alert queues

Alerts are generated by the Rule Engine and by ACE and Fractals offers a flexible, configurable mechanism for handling such alerts.

Fractals implements the concept of an alert group which provides a way of grouping alerts which meet common selection criteria. Such criteria include, for example, fraud score, product type & transaction amount.

Each analyst has his or her own alert queue but an alert queue can be linked to several alert groups to provide a high degree of configurability to meet operational needs.

Fraud Analysts Workbench

Fractals provides a powerful browser-based capability for processing alerts which enables fraud analysts to interrogate the reporting database and fully understand cardholder and merchant patterns of behaviour.

Versatile product

Fractals is available in a range of afffordable packages designed to suit the individual needs of issuers, acquirers and processors in the retail payments business, starting with rules-only systems and ranging up to high performance ACE-based intelligent detection systems.

Fractals Fast Facts

- ✓ Unified framework for issuer and acquirer, debit and credit card fraud detection
- ✓ Browser-based GUIs
- ✓ Powerful Rules Engine enables point-&-click creation, evaluation and deployment of user-defined detection rules, without coding
- ✓ Adaptive Classification Engine (ACE) produces intelligible, intelligent alerts
- ✓ Continuously optimal detection performance via self adaptive, self optimizing strategies
- ✓ Can incorporate 3rd party alerts
- ✓ Cost effective real time integration with authorization and acquiring systems
- ✓ PABP PCI DSS certified
- ✓ Operates in real time, near real time and batch
- ✓ Provides specific detection strategies customised to usage and fraud patterns
- ✓ Suitable for single or multi-bank operation, hence ideal for processors
- ✓ 100% Java, runs on UNIX, Linux and Windows operating systems and, *inter alia*, Stratus, IBM, Sun and HP hardware

Email: sales@alaric.com
Website: www.alaric.com

London Office
Telephone: +44 (0) 207 593 2200
Kuala Lumpur Office
Telephone: +60 (0)3 2287 7410
Melbourne Office
Telephone: +61 (0)3 8610 6494
Ocean, NJ Office
Telephone: +1 732 481 2142