

# FRACTALS ACE

## Adaptive Classification Engine

**Fractals ACE (Adaptive Classification Engine) complements the Fractals Rules Engine to deliver industry leading, self adaptive, intelligent card fraud detection.**

### Intelligent fraud detection

ACE is a major component of Fractals which operates separately from, but simultaneously with, the Rules Engine. It 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 rules capability, can deploy ACE standalone.

### ACE in production

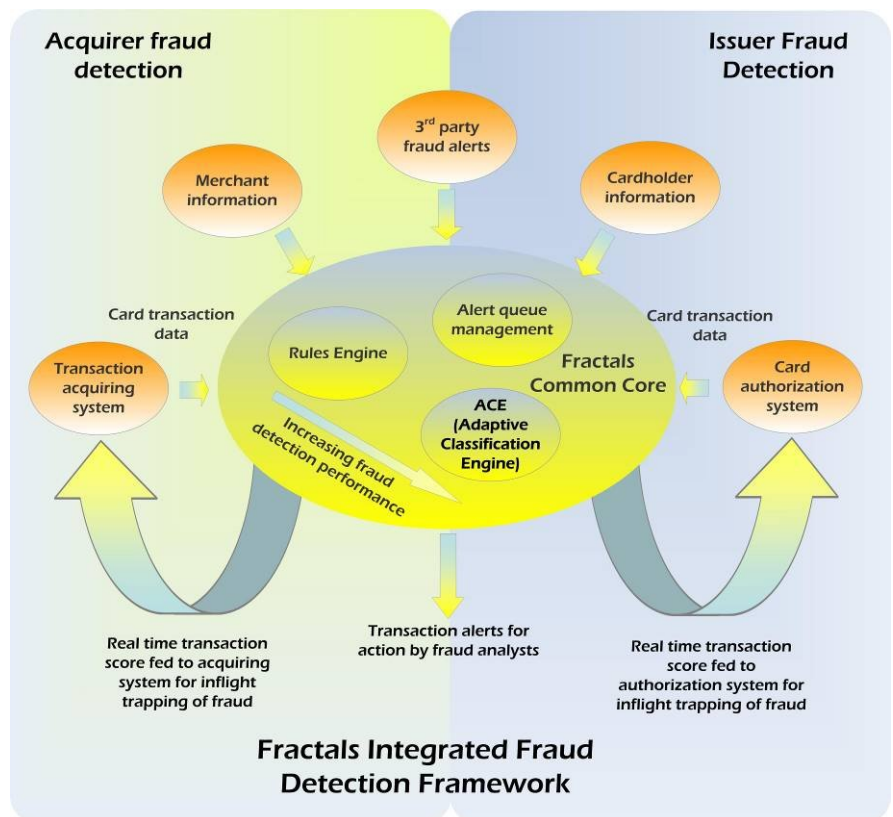
ACE generates fraud alerts by executing mathematical models against incoming transactions to produce a fraud score or "probability of fraud".

Typically in production, ACE regularly detects between 55-80% of all fraud cases whilst delivering a manageable set of alerts for fraud analysts to work through. This is provided automatically by ACE, and does not include fraud detected by user specified rules.

### ACE benefits

In operation, ACE provides significant benefits to an organization and major advantages over neural network or purely rules based detection models.

ACE is *highly accurate* and provides a *customized detection model* based on the institution's own transaction data. Customized models provide better results than generic models that use consortium or sampled transaction data because they are derived from an institution's own fraud patterns.



ACE *identifies new patterns of fraud* and maintains its detection effectiveness through a regular recalibration which can be performed as often as the institution wishes.

Moreover, ACE models *can self adapt and self optimize between model recalibrations* to ensure continuing high detection rates. This contrasts with neural methods, the performance of which drops off substantially between model retrains.

ACE provides good results for both *large* and *small* cardbases.

Strategies within ACE can be created and calibrated for *specific card types* within an issued card portfolio to further improve detection effectiveness. For instance, a particular type of card may have high credit limits and may be subject to a high level of fraud and therefore may require a separate, specific detection model to improve

fraud detection rates for that product.

ACE produces *alerts that can be understood* by its users. Therefore the institution can understand why a transaction has been alerted as a fraud by the detection model.

ACE is *highly flexible* and can include third party alerts or additional data items as part of its scoring mechanism.

ACE can also *include the institution's own fraud scoring models* as part of its scoring mechanism and can therefore form the core modelling component of an institution's own internal development programme.

The false positive rate of ACE can be adjusted to deliver the *number of alerts* which are capable of being handled by the available number of fraud analysts.

ACE offers *online real-time scoring* and can provide an institution with a real-time



review of fraud scores and an in-flight fraud prevention capability for referring and declining transactions.

### ACE for a specific customer

For a specific customer, the ACE model is configured via automated analysis of historical transaction data.

The ACE model is initially calibrated using a dataset that contains a customer's historical transactions with frauds tagged to enable ACE to recognize the fraud patterns present in this data.

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

ACE's probabilistic foundation means that it can be recalibrated very rapidly, whenever new transaction data is available. Recalibration takes a matter of hours and can be performed on-site, on the customer's computers without data having to leave the customer's premises. This means that it is economically viable to recalibrate ACE on a frequent basis, thereby maintaining optimal detection effectiveness.

This represents a marked advantage over the iterative, slow and expensive modelling techniques employed by neural networks.

### Serving the middle market

ACE makes very efficient use of the training dataset and requires less data to calibrate its models than comparable neural network solutions.

This means that, as well as being able to cope with the needs of the largest institution, ACE is able to produce quality

detection models for small to medium sized card bases. Thus, for the first time, medium-size players can deploy accurate, custom statistical fraud detection models at an economical price.

### Real time integration

Fractals/ACE may be readily deployed together with Alaric's Authentic issuer/acquirer product and integrated for real time operation.

However, Fractals can also be used in conjunction with third party issuing and acquiring 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 real time integration with the client's systems.

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.

### Technology platform

ACE is written in Java and therefore supports a wide range of hardware platforms.

It can be deployed in a *multi-institution mode*, making it ideally suited to processors and service providers and can also operate in a *multi-product mode* for an institution with multiple card products, enabling detection models to be deployed which are tuned for optimal performance at the card product level.

ACE's Java-based architecture is highly scalable and requirements for high volume throughput can be by met simply by adding more

hardware and by distributing ACE across multiple processors and/or multiple computers.

### Summary

ACE offers institutions improved flexibility, accuracy and cost-effectiveness in their fraud detection processes and provides an easy migration path to an online real-time (in-flight) fraud prevention capability.

#### Fractals ACE Fast Facts

- ✓ Unified detection engine for issuer and acquirer, debit and credit card fraud detection
- ✓ Produces intelligible, intelligent alerts
- ✓ Fast, economical model training
- ✓ Continuously optimal detection performance via self adaptive, self optimizing strategies
- ✓ Can incorporate 3<sup>rd</sup> party alerts
- ✓ Cost effective real time integration with authorization and acquiring systems
- ✓ Requires less data than neural networks, so can offer custom intelligent modelling for mid-size card bases
- ✓ 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

