Fraud Transaction Monitoring

Manage fraud risk in real-time with a platform trusted by Tier 1 banks

Improve transaction monitoring, minimise card risk and prevent fraud attacks in real-time using machine learning and behavioural analytics.

Going live with a card program requires a fraud monitoring solution with sophisticated detection models that query large sets of data over a period of time. The Fraud Transaction Monitoring system (powered by Featurespace) is a best-in-class, flexible card fraud solution that minimises online and offline card risk and offers real-time detection of card fraud.

Using adaptive behavioural analytics and machine learning, Enhanced Fraud Transaction Monitoring adapts to new fraud types and identifies unknown threats by detecting unexpected changes (anomalies) in real-time data. This improves transaction monitoring, identifies fraud and reduces the number of occurrences where legitimate transactions are flagged as suspicious, payments are stopped or accounts locked.

Features

Fraud Transaction Monitoring

- **Real-time monitoring** – Covers both financial and non-financial events.
- **Industry accepted event formats** – Card schema based on ISO 20022 messaging format standards.
- **Instant decisions and processing** – Best-in-class analytical models manage complex fraud attacks in real-time (average of 30 milliseconds).
- **Prevent fraud** – Mark an event as suspicious, highlight the event, send an email notification and block the card.
- **One integrated solution** – Management console provides instant visibility through a clear colour-coded dashboard.
- **Adaptive rules engine** – Award-winning machine learning identifies risk in real-time and automatically protects against evolving fraud threats.

Enhanced Fraud Transaction Monitoring

All of the above, plus:

- **Self-tuning models** – Models automatically retune, eliminating the need for updates.
- **Adaptive behavioural analytics** – Award-winning machine learning spots bad actors in real-time and automatically protects against evolving fraud threats.

Add-Ons

- **Sandbox Replay** – author new rules and thresholds and test the impact of these changes before going live.
- **Customer Fraud Alerts** – send an SMS to your customer when you decline a transaction.
- **Scam transaction monitoring** – to identify potential scam transactions.
- **Fully managed service option** – to reduce operational overhead.

Benefits

- **Accelerated Go To Market** – pre-integrated solution only requires configuration to go live.
- **Economies of scale** – leverage Thredd's transactional volumes to reduce the costs of the solution.
- **Enhanced control** – using an anti-fraud rules engine designed to protect transactions.
- **Attract and retain** – an enhanced value proposition to draw customers in and keep them.
- **Early detection** – reports and alerts identify actions you could take to reduce fraud.
- **Effortless protection** – proactively manage incidents of fraud on behalf of your customers.
- **Reduce financial risk** – flag suspicious transactions or events which are predefined by a set of rules.
- **Ease and convenience** – transaction monitoring capabilities and statistical calculations of historical data.
- **Expert support** – support and guidance on the rules that best mitigate against fraud.
- **Trust and assurance** – knowledge that your account is constantly monitored for any suspicious activity.
- **Lower Operational Costs** – Instinctively understands fraud risk through adaptive behavioural analytics, minimising alerts, declines and manual review.

How It Works

Fraud Transaction Monitoring

Fraud Transaction Monitoring uses behavioural analytics to detect and prevent fraud with machine learning software that monitors individuals' behaviour and detects anomalies to identify risk and prevent fraud attacks in real-time.

Fraud Transaction Monitoring			
Instant decisions and processing	**Intuitive UI**	**Quickly create & deploy rules**	**Adaptive rules engine**
Best-in-class analytical models manage complex fraud attacks in real-time (average of 30 milliseconds)	Easy and intuitive case management with a range of workflows to suit your needs	Wizard allows for rules to be made in minutes, deployed in seconds	Build rules and models customised for your environment and specific data sets, namely high net worth vs financial inclusion

We'll start you off with a set of rules that we've tried and tested. These rules will protect your business from most fraud attacks.

Best-in-class analytical models manage complex fraud attacks in real time (average of 30 milliseconds).

You can customise the Do-It-Yourself dynamic analytics by adjusting the model alert thresholds, writing, testing and deploying rules. We also provide a sandbox environment for your testing against historical and production data.

Explainable	**Product**	**Documentation**	**Do-It-Yourself Dynamic Analytics**
• Easy to understand reason codes on model outputs • Reason codes tailored for each use case • Easily see which groups of features contributed to an alert	• Extensive model and rule performance reporting • Robust governance controls around model retrains • Standard schema based on ISO20022 messaging format • Full auditability • Support in line with SR11-7 guidance	• Procedure documentation • Sample standard docs • Documentation to meet supervisory and regulatory requirements	• Write, test and deploy rules • 4 eyes approval process

The adaptive rules engine deploys adaptive behavioural analytics in real-time for sophisticated evolving rules to be authored and configured by your risk analysts.

The enterprise-class rules engine builds rules against any data type, variable or event and is able to use behavioural features based on state to spot small anomalies in customer behaviour in real-time. It uses the analytical work-flow manager to build complicated nested rules.

Enterprise-class rules engine

- Build rules against any data type, variable or event

- Able to use behavioural features based on state to spot small anomalies in customer behaviour in real time

Quickly create and deploy

- Wizard allows for rules to be made in minutes, deployed in seconds

- Empowers fraud analysts to build comprehensive rule sets aggregating values over time to create variables, e.g., average spend over last week

- Use code to create rules, or enter rules in an editor without using code.

Easily modify and maintain

- Change messages to downstream systems and actions instantly using tag values

- Test rules instantly using sandbox replay, no guessing

- Instant roll back to previous versions of ruleset

- Manage callouts to third parties

- 4 eyes approval process

Rules are created in minutes and deployed in seconds. Your fraud analysts can build comprehensive rule sets aggregating values over time to create variables, for example the average spend over the previous week. Using code to create rules, the rule editor enables rule creation without having to manually create code. For easy modification and maintenance, you can instantly change messages to downstream systems and actions, using tag values. You can also test the rules instantly using sandbox reply and immediately roll back to previous versions of the rule set. For easy modification and maintenance, you can instantly change messages to downstream systems and actions, using tag values. You can also test the rules instantly using Sandbox Replay and immediately roll back to previous versions of the rule set.

Enhanced Fraud Transaction Monitoring

To minimise card risk both online and offline, enhanced Fraud Transaction Monitoring uses real-time machine learning with adaptive behavioural analytics, anomaly detection, and expert rules and models. It offers automatic detection of fraud, zero model degradation (no retuning required) and focuses on genuine behaviour, reducing false positives.

Enhanced Fraud Transaction Monitoring

Self-tuning models	Lower operational costs	Adaptive behavioural analytics
Models automatically retune eliminating the need for updates	Instinctively understand fraud risk through adaptive behavioural analytics minimising alerts, declines and manual review	Award-winning machine learning spots bad actors in real-time and automatically protects against evolving fraud threats

Enhanced Fraud Transaction Monitoring also analyses the degree a customer's genuine behaviour deviates from the usual behaviour.

Indicators	
	Credit Card
	Debit Card
	Card-Not-Present
	Card Present
	Bank Transfer
	Mobile Bank Transfer
	Application
	E-Commerce
	Digital Money
	E-Wallet
	Prepaid Card

Enhanced Fraud Transaction Monitoring Profile of Genuine Customer Behaviour

Genuine Behaviour
For customer 0001

Customer 0001

Extent to which customer exhibits behaviour

Anomaly — Usual — Anomaly

Indicators: 1, 2, 3, 4, 5, 6

To determine whether a transaction is anomalous, it must be viewed in context. Enhanced Fraud Transaction Monitoring applies context to human behaviour.

Anomalous Transactions

Example customer transaction

Value
Online purchases of high value

Location
Made in UK from vendor

Time
At 2:00am UK time

- Suspicious?
- Every transaction must be viewed in context of the customer's historical transaction activity over time.
- This context is captured in the customer's behavioural profile.

Enhanced Fraud Transaction Monitoring Profile of Genuine Customer Behaviour

Genuine Behaviour
For customer 0001

Extent to which customer exhibits behaviour

Anomaly | Usual | Anomaly

Enhanced Fraud Transaction Monitoring provides the benefits of speed and accuracy of fraud detection, together with the enhanced power of adaptive learning.

Speed	Accuracy	Adaptive
Real-time decisions and configurable analytics	**Catch more fraud, reduce false positives, lower overheads, and increase genuine customer acceptance**	**Maintains detection and accuracy as trends change**
99.9%	Average Value Detection Rate improvement of 50%	Automatically detects new types of fraud
Of auths are assessed <100ms		Dramatically reduces the number of false positives
Rule library and machine learning model for card fraud tactics		Zero model degradation – no retuning required
<60sec		
to spot a master attack		

Scam Transaction Monitoring (add-on)

Scam Transaction Monitoring provides enhanced fraud protection on top of existing fraud controls – tracking the fraud missed by banks that evades existing defences. The solution offers maximum protection with minimal investment, working out-of -the-box from day one, offering a solution that keeps you ahead of changing PSR regulations, saving time and saving money. Features:
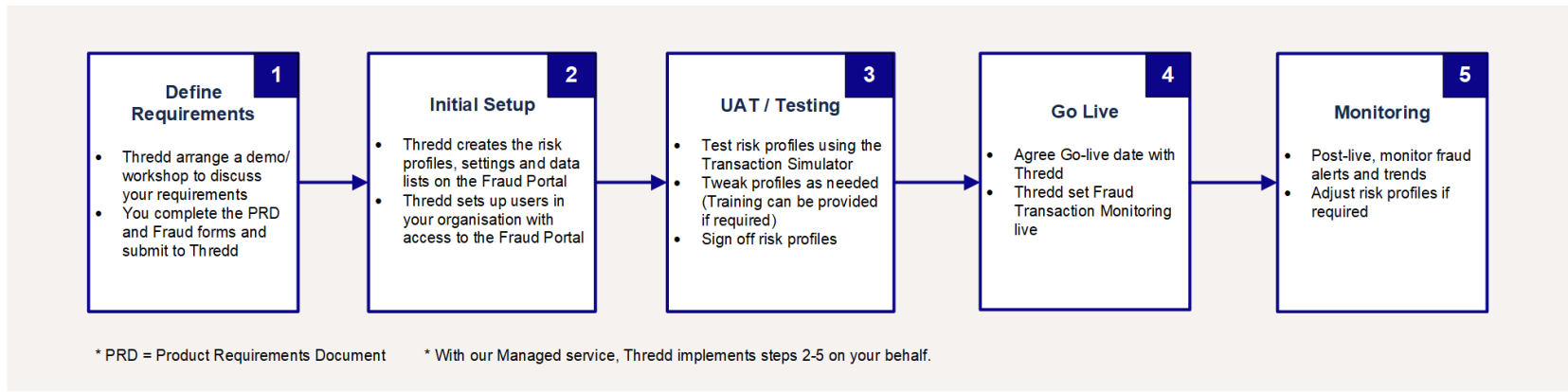
- Works without historical data
- Requires no sensitive data - only the payment message
- Monitors inbound and outbound payments

You can purchase Scam Transaction Monitoring as an add-on to Fraud Transaction Monitoring, or as a standalone purchase. For more information contact your Account Manager.

Setup At-a-Glance

Below is a high-level view of the setup steps.

Define Requirements	1		**Initial Setup**	2		**UAT / Testing**	3		**Go Live**	4		**Monitoring**	5

1 — Define Requirements
- Thredd arrange a demo/ workshop to discuss your requirements
- You complete the PRD and Fraud forms and submit to Thredd

2 — Initial Setup
- Thredd creates the risk profiles, settings and data lists on the Fraud Portal
- Thredd sets up users in your organisation with access to the Fraud Portal

3 — UAT / Testing
- Test risk profiles using the Transaction Simulator
- Tweak profiles as needed (Training can be provided if required)
- Sign off risk profiles

4 — Go Live
- Agree Go-live date with Thredd
- Thredd set Fraud Transaction Monitoring live

5 — Monitoring
- Post-live, monitor fraud alerts and trends
- Adjust risk profiles if required

* PRD = Product Requirements Document   * With our Managed service, Thredd implements steps 2-5 on your behalf.

Setup Options

We offer a number of different service options for the Fraud Transaction Monitoring system. For more information, please discuss with your account manager.

Fraud Transaction Monitoring

Feature	Fraud Transaction Monitoring (FTM)	FTM + Sandbox Replay + Customer Fraud Alerts	Fraud Transaction Monitoring Service
Real-time fraud detection	√	√	√
Adaptive rules engine	√	√	√
Sandbox Replay	X	√	√
Customer Fraud Alerts	X	√	√
Managed service	X	X	√
Scam transaction monitoring	√	√	√

Enhanced Fraud Transaction Monitoring

Feature	Enhanced Fraud Transaction Monitoring (EFTM)	EFTM + Sandbox Replay + Customer Fraud Alerts	Enhanced Fraud Transaction Monitoring Service
Real-time fraud detection	√	√	√
Real-time risk-based scoring decisions	√	√	√
Adaptive rules engine	√	√	√
Adaptive behavioural analytics	√	√	√
Self-tuning models	√	√	√
Sandbox Replay	X	√	√

Feature	Enhanced Fraud Transaction Monitoring (EFTM)	EFTM + Sandbox Replay + Customer Fraud Alerts	Enhanced Fraud Transaction Monitoring Service
Customer Fraud Alerts	x	√	√
Managed service	x	x	√
Scam transaction monitoring	√	√	√

FAQs

Q. Is fraud monitoring required for regulatory compliance?

Fraud monitoring, like having a team analysing authorisations 24/7, isn't a regulatory compliance, but there are other regulations designed to prevent fraud, where Fraud monitoring can help with your compliance.

Q. What is Fraud Transaction Monitoring?

A solution which provides real-time fraud detection and transaction control using tried and tested fraud rules.

Q. What is real-time fraud detection?

Real-time means making an assessment on a transaction while it is still happening, before deciding to approve or decline it.

Q. Can I add rules to the pre-set ones?

Yes. And you can manually add new rules and change the settings and event data in any existing rules.

Q. What is Enhanced Fraud Transaction Monitoring?

It gives you everything Fraud Transaction Monitoring does but with machine learning to change the event data built into your fraud rules. It sets and re-sets its own parameters, so you don't have to. It also gives authorisations a risk score, in real-time. You can use these scores to optimise your fraud rules, helping you to stay ahead of fraud.

> **Note:** This feature is available to customers with large transaction volumes. For details, please speak to your Thredd account manager.

Q. What is Sandbox Replay?

Sandbox Replay is a test environment where you can optimise the rules and event data you have live, without touching your live environment.

Q. What if my sandbox is outperforming your live environment?

You can push the rules in your sandbox to your live environment.

Q. How long can implementation take?

Because it's already built in our platform, all you need to do is tell us what rules you want to go live with. It can be as little as two weeks. But this depends on how quickly you can give us the information we need.

Q. Can you help set up my rules?

Yes, as part of the implementation, we start you off with a set of 18 base rules, which already include statistics on customer profiles we have. If you take our managed service, we will also set up and configure a set of tailored rules on your behalf.

Q. Where can I find out more?

For more information, refer to the Transaction Monitoring System Guides or contact your Account Manager.

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd UK Ltd.

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.