

T-NEX Fraud Detection: transaction monitoring and case management

Brief version: 1.0 · 11 September 2026

Documented functional state: 30 August 2026 · Application version 15.23.0

T-NEX Fraud Detection helps financial institutions identify unusual transaction patterns, group alerts by customer and document professional decisions. It combines configurable rules, supporting transactions, AI-assisted triage and an audit trail for case handling.

Anti-money-laundering monitoring and card or payment fraud are treated as distinct areas of work. The module **detects and records**. It does not block payments or cards.

Documented functionality

Area	Supported work
Transaction intake	Receiving transactions through an interface and detecting duplicates using the external transaction identifier
Rules	Nine documented typologies with configurable parameters, including structuring, rapid throughput and unusual card frequency
Alerts	Recording the trigger, category, severity and supporting transactions
AI triage	Risk score, rationale and recommended action, with model and prompt-version identification
Case management	Grouping a customer's alerts, assigning ownership, setting status, commenting and escalating
Closure	Reasoned closure or documenting a suspicious transaction report draft
Rule evaluation	Testing against historical transactions; AI rule suggestions initially saved as disabled drafts

Inputs and data quality

Required data includes stable external transaction and customer identifiers, account and currency, amount, booking time, channel, counterparty and country. Card transactions also include the last four card digits and the capture method. Customer context includes the KYC risk band.

Timestamps, country fields and identifier uniqueness are material to the analysis. Changing identifiers create duplicates; incorrect time zones distort time-window rules. Delivery speed must match the period being evaluated. Source systems and acceptable delivery delays are determined for the specific deployment.

Example: incoming funds transferred onwards rapidly

1. The interface receives transactions and updates the evaluation context.
2. A configured rule identifies the pattern and creates an alert containing the relevant transactions.
3. AI triage adds a reasoned assessment and recommendation; alerts are grouped into a customer case.

4. The analyst checks the customer profile, counterparties, timing and documented explanations.
5. The analyst records a justified closure, escalates the case or prepares a report draft. The reasoning remains in the audit trail.

This schematic workflow uses no real customer data. An alert or high AI risk score does not establish fraud or money laundering. Decisions remain with the responsible professionals. Reports are submitted separately through the designated reporting system.

Roles and AI oversight

Four permission areas separate reading, case handling, rule management and administration. During implementation, these are mapped to the institution's actual responsibilities. Read access allows review of case files and audit trails without permitting case changes.

Triage uses the central AI service of the T-NEX platform. The model and prompt version are recorded with the assessment. If AI is unavailable, the alert remains actionable with rule-based fallback text, identified by the .fallback suffix in the prompt version. Analysis can be rerun after the service is restored.

Analyst review explicitly includes implausible AI reasoning and differences between a recommendation and the analyst's decision. Model selection, data flows, provider terms and permissions form part of the agreed operating configuration.

Calibration before and after implementation

A backtest evaluates a rule against historical transactions without automatically generating new alerts. The number of transactions checked, matches, match rate and distribution over time help assess relevance and workload. Matches also require substantive review. A match rate alone is not a measure of precision or effectiveness.

AI rule suggestions are saved as disabled drafts, reviewed by specialists and tested against historical data. Activation follows a separate decision. Rule versions and reasons for changes should remain traceable. Thresholds and handling deadlines must fit the institution; this brief does not prescribe universal settings.

Integration, operation and procurement

The module is enabled within the T-NEX platform and requires data integration, appropriate permissions and a configured AI service for AI triage. Its documented simulator is intended for separate training, demonstration and acceptance environments. It writes synthetic records into the module tables and must not be mixed with production data.

To be agreed in the proposal	Specific decisions
Functional scope	AML, card/payment fraud, typologies, responsibilities and escalation paths
Data integration	Sources, field mappings, customer records, duplicate detection and delivery delay
AI	Provider, model, data flows, approvals and service-failure procedures
Implementation	Separate test environment, historical test data, calibration and analyst training
Operation	Target environment, access, monitoring, backup, restoration and release management

To be agreed in the proposal	Specific decisions
Contractual scope	Licence, implementation, support hours, response commitments and required evidence

The functional documentation does not determine the hosting, data-protection or service agreement for a particular deployment. The module also does not replace the institution's organisational decisions or reporting procedures.

Evidence basis

This brief summarises the functional handbook dated 30 August 2026. The version identifies the documented application. The handbook is not an independent effectiveness assessment and does not establish a guaranteed detection rate, availability level or certified regulatory suitability. A production customer deployment is not inferred from the module description.

[Product and workflow](#) · [Evidence for institutions](#)

Contact: info@t-nex.de