Manipulation Risk Monitoring and High Risk Entity List

Stop manipulation fraud before it impacts customers and operations. Strengthen trust by protecting vulnerable customers from sophisticated manipulation.

Banks increasingly face sophisticated social engineering threats, manipulated customers, and cross-bank fraud patterns. To counter this, Manipulation Risk Monitoring (MRM) and the High-Risk Entity List (HREL) provide real-time intelligence, behaviour based detection, and controlled measures to prevent losses and protect vulnerable customers. In this context, manipulation fraud refers specifically to the manipulation of the payer.

The Customer Challenge

- Customer initiated manipulation fraud is increasing significantly.
- High false positives and limited follow-up capacity make 24/7 monitoring difficult.
- Manipulated customers may continue fraudulent payments across channels and banks if protection is not coordinated.
- Customers expect protection even when they are initiating the payment themselves.
- Regulators expect stronger, proactive controls for manipulation, and faster reporting of suspicious activity.

Our Solution

Two complementary fraud prevention products

Manipulation Risk Monitoring (MRM)

A behaviour based monitoring service that focuses on for example high risk Merchant Category Codes (MCC) and identifies victims of manipulation fraud through behavioural analysis, pattern recognition, and real time monitoring.

Optional Payment Service User (PSU) follow up with questionnaire.

High Risk Entity List (HREL)

A list of customers at risk of manipulation fraud, managed by the bank. When a customer is added, Tieto enforces stricter controls to prevent suspicious outgoing payments cross channels.

Together, MRM helps detect manipulation fraud early, while HREL helps protect customers already identified as high risk.

Value Benefits

- Early detection of manipulation behaviour before fraudulent transactions are completed.
- Reduced losses by rejecting suspicious outgoing payments.
- Stronger customer protection for individuals known to be manipulated or vulnerable (HREL).
- Structured customer communication and documentation of Social-Engineering fraud cases with the PSU Follow-up with questionnaire option. Reduces risk for loss, reputational damage and legal disputes.

Key Use Cases

- Retail and corporate banking fraud mitigation
- Real time monitoring for transactions
- Structured documentation of customer communication

Integration & Delivery Model

- Modular adoption: MRM only, HREL only, or combined
- HREL can be delivered standalone; PSU Follow up requires MRM Basis.

Business Outcomes

- Measurably reduced losses related to manipulation fraud
- Lower operational workload
- Faster fraud detection
- Stronger compliance posture
- Higher customer trust and reduced reputational risk

Strong documented results
from pilot banks using MRM

Restrictions via HREL **significantly reduce exposure to Manipulation Fraud** while being able to maintain the customer relationship

4.26 billion
transactions processed and monitored annually

> 90%
Fraud Detection Rate

Trusted by more than 75 institutions across Europe

24/7/365
Investigation

Ready to strengthen your fraud prevention capabilities?

Contact your customer manager or **servicedesk.fcp@tieto.com**