Pre- vs Post-Transaction Monitoring and Detection Rules

Jeremy Zarb, Jeremy Mercieca Abela and Elena Tabone

Enforcement Section

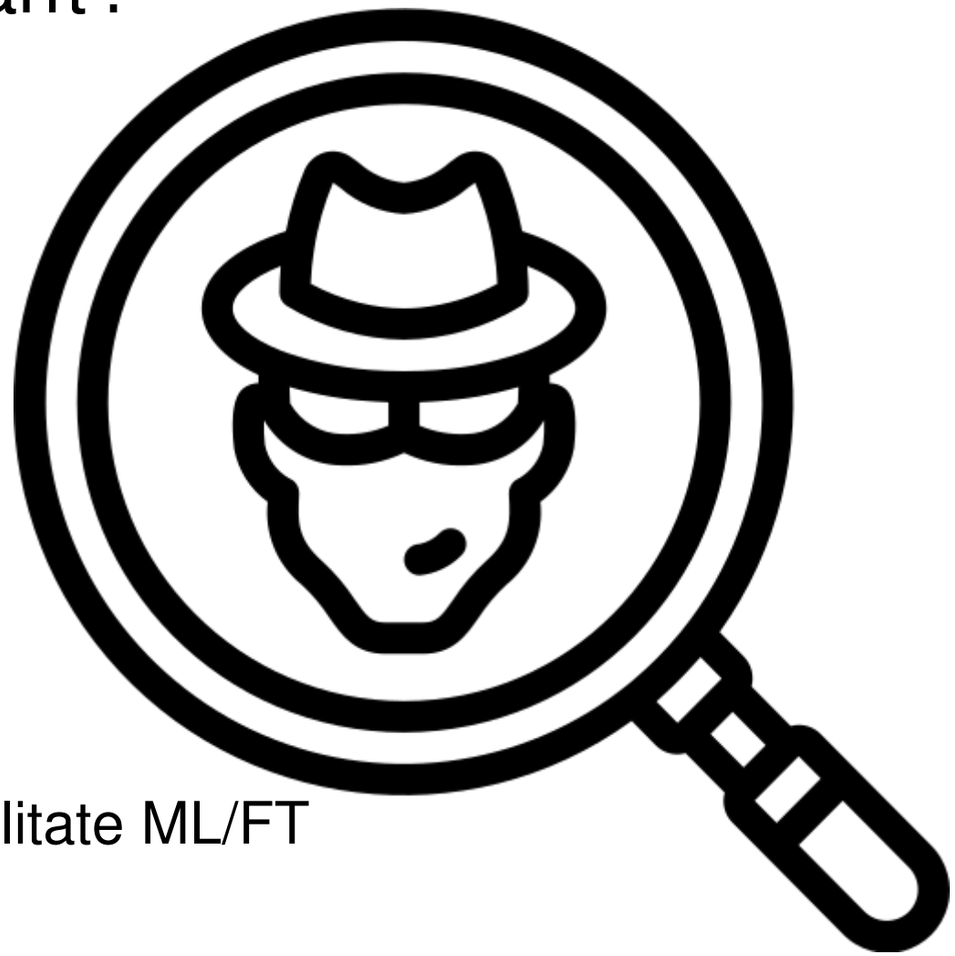
Training Session on Transaction Monitoring

6th June 2023

Detection Rules: Implementation and Testing

Why are Detection Rules important?

- ❑ Risk Identification
- ❑ Automation & Efficiency
- ❑ Scalability& Consistency
- ❑ Effective to Prove Compliance
- ❑ Customization & Adaptability
- ❑ Minimize the possibility of being used to facilitate ML/FT



Detection Rules: Risk Based Calibration

One Size Fits All

Calibrated

Example #1: Shortcomings of a One Size Fits All System

Transactions flagged if:

Product

- Card spending
- **€15k** (1 transaction)

Frequency

- > 5 transactions within the same day
- > 30 transactions within a month.

Industries

- High Risk Merchant Category Codes (MCCs)

Risky countries

- High risk Countries

Example #1: Risk Based Calibration

John

Finance Officer

Annual Income: **€60k**

Expected Spending: **€10k per year**

Product
- Card spending
- **€15k** (1 transaction)

Frequency
- > 5 transactions within the same day
- > 30 transactions within a month.

Industries
- High Risk Merchant Category Codes (MCCs)

Risky countries
- High risk Countries

6 months

20 transactions of €1k each per month + Low risk MCCs + Medium Risk Countries = **€120k**

4 considerations to implement effective calibrated risk-based detection rules

1) Business Model

- ❑Understand the nature of your business model, including the products or services offered, revenue streams, and the overall industry you operate in.

2) Customer Base

- ❑Demographics, geographic location and risk profiles
- ❑E.g.: individuals, businesses, high-risk clients, etc.

3) Transaction Channels

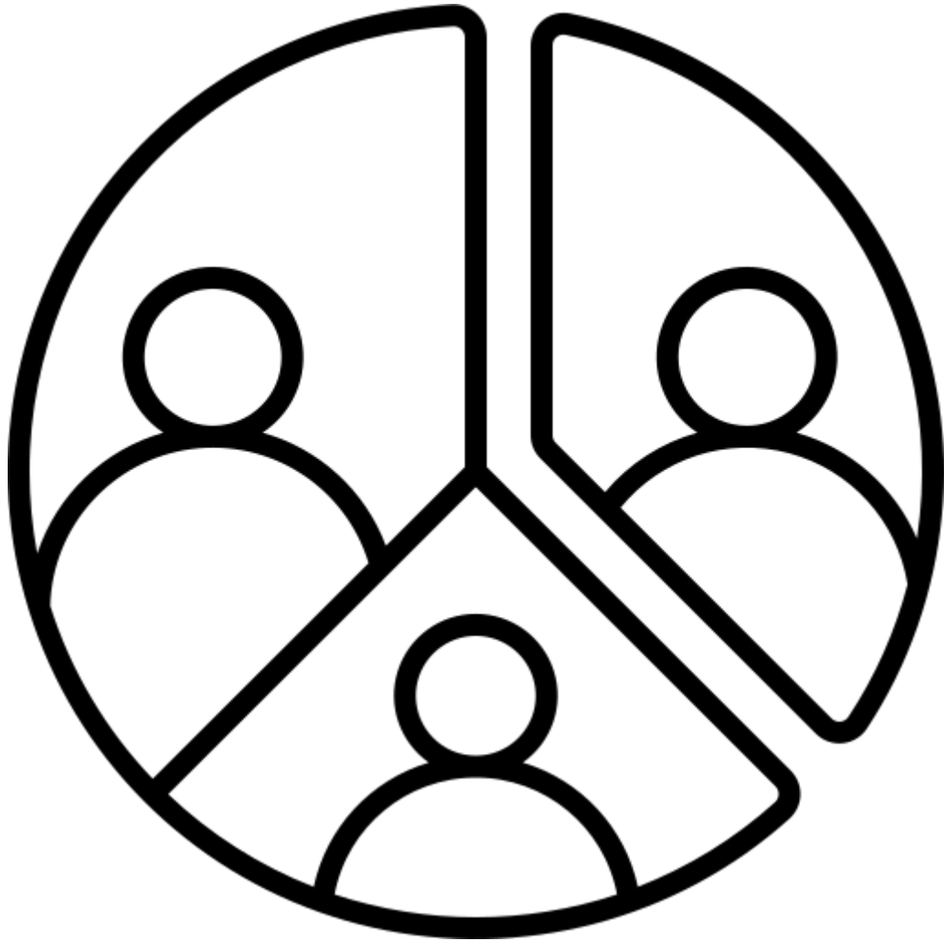
- ❑Identify the various channels through which transactions occur in your business.
- ❑E.g.: Cash, online platforms, mobile applications, third-party payment processors, etc.

4) Historic transaction activity

- ❑Analyse historical transaction data to identify patterns, trends, and anomalies.

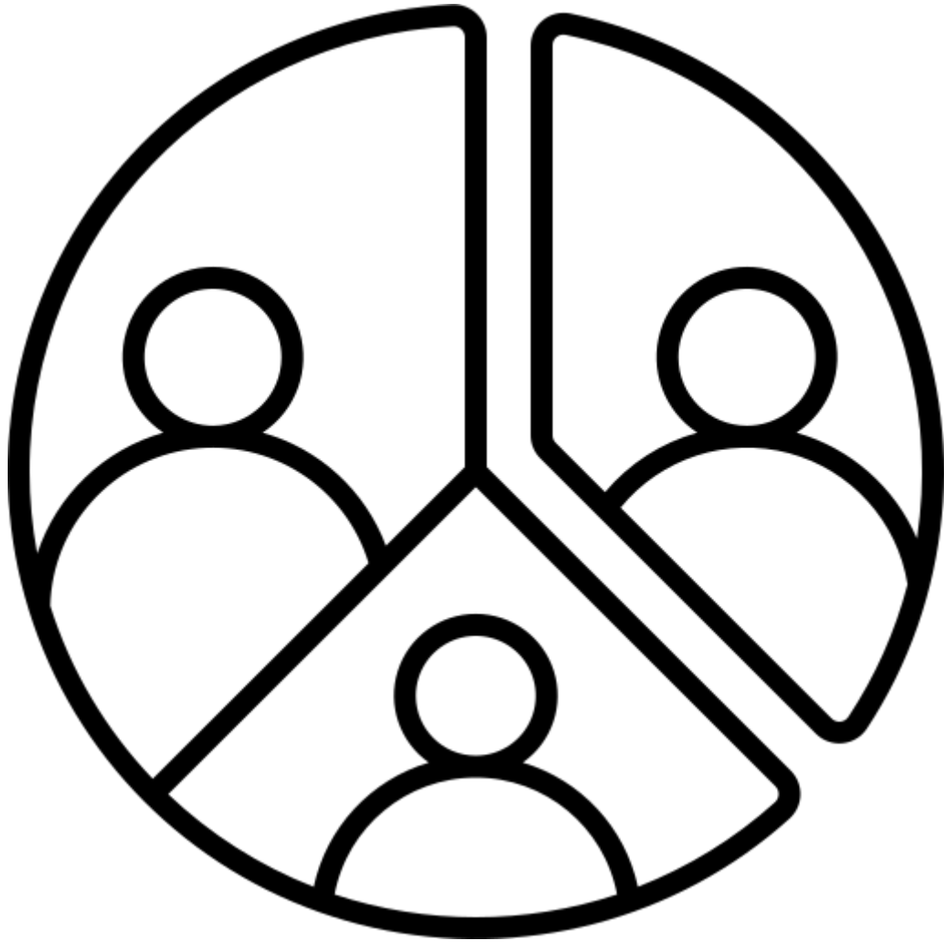
Detection Rules: Customer Segments

Personal Customers
Employed individuals ❑ Full/part-time and seasonal employees ❑ Professionals / public sector / blue collar workers
Self-employed individuals ❑ Small business owners ❑ DNFBPs
Low/no income individuals ❑ Unemployed ❑ Pensioners ❑ Students
Higher risk customers ❑ Politically exposed persons (PEPs) ❑ High Net Worth (HNW) individuals ❑ Non-resident customers



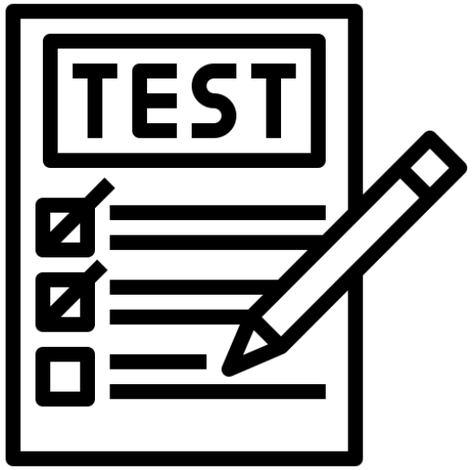
Detection Rules: Customer Segments

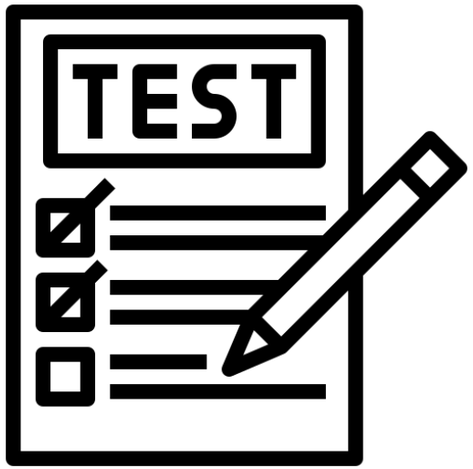
Corporate Customers
Size of business and operations ❑ Small/ Medium/ Large-sized enterprises
Business structure ❑ Private and public companies ❑ Other legal arrangements ❑ Governmental entities
Economic sector - Primary/ Secondary/ Tertiary/ Quaternary
Industry and product risk - Cash intensive businesses - High risk products - Foreign financial institutions - Correspondent banking relationships
Transactional activity - Average transaction value and volume



Why do we need to TEST the rules established?

- ❑ Accuracy & Effectiveness
- ❑ Customization & Flexibility
- ❑ False Positive Reduction
- ❑ Performance Optimization
- ❑ Continuous Improvement





=

Efficient use of resources

Customer experience not adversely impacted

Efficient & Accurate identification of suspicious transactions

Types of Tests

Back Testing

- Evaluate the performance and effectiveness of a transaction monitoring system by applying it to historical data.

Above the line (ATL)

- Testing the system's detection capabilities using synthetic or simulated transactions that are deliberately designed to trigger the monitoring rules.

Below the line (BTL)

- Assessing the system's performance in identifying and handling legitimate or low-risk transactions, ensuring they are not incorrectly flagged as suspicious or generating false positives.

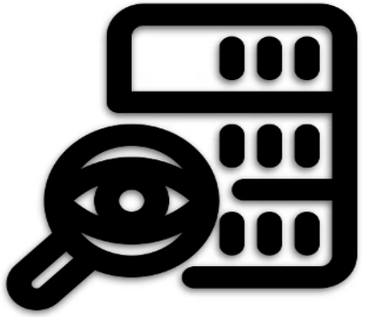
Detection Rules: Final Recommendations

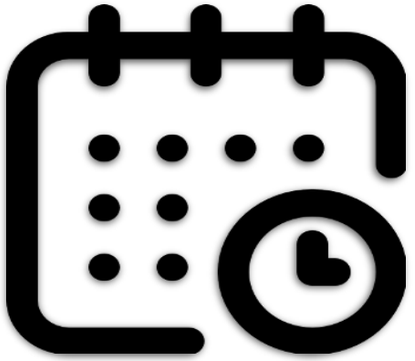
Audit Trail

- Critical to demonstrate SPs efforts to establish an effective and compliant transactional monitoring system.

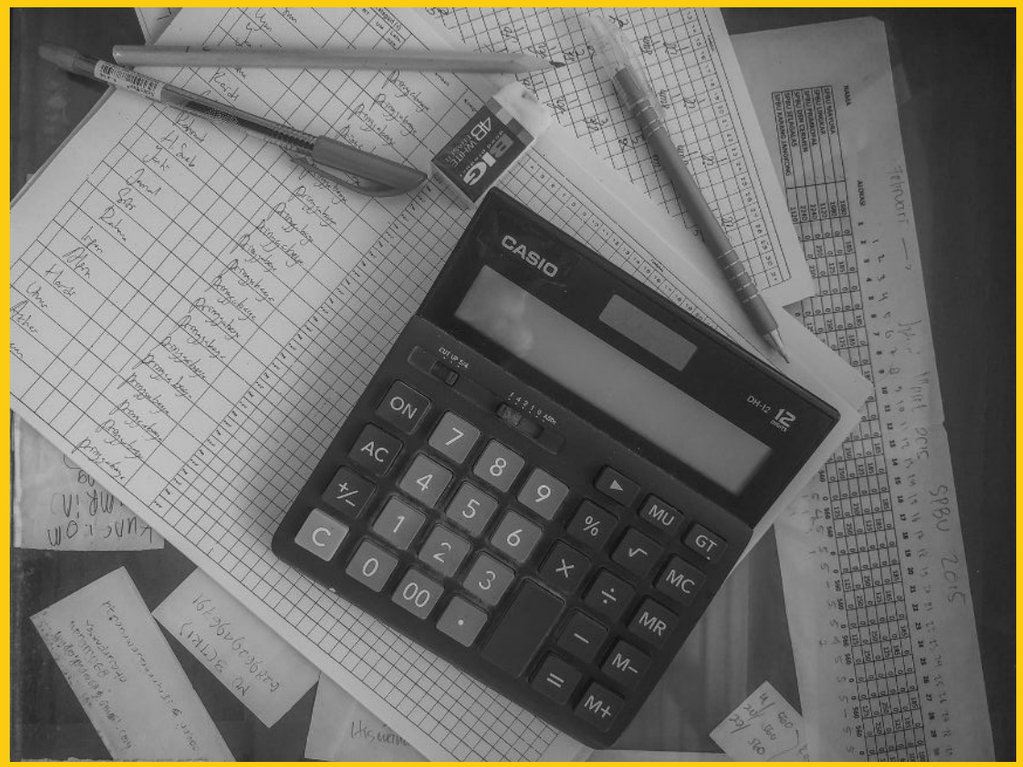
Periodical Checks

- Assess performance, optimize detection rules, monitor compliance, ensure data quality, maintain system integrity and prepare for audits.





Pre-transaction Monitoring and Post-transaction Monitoring



Pre-Transaction Monitoring

What is Pre-Transaction Monitoring?

- Monitoring activities that are carried out in real time prior to a transaction being executed.
- Pre-transaction monitoring facilitates the timely detection of unusual or suspicious transactions before they are affected and reduces the risk of ML/FT materialising.

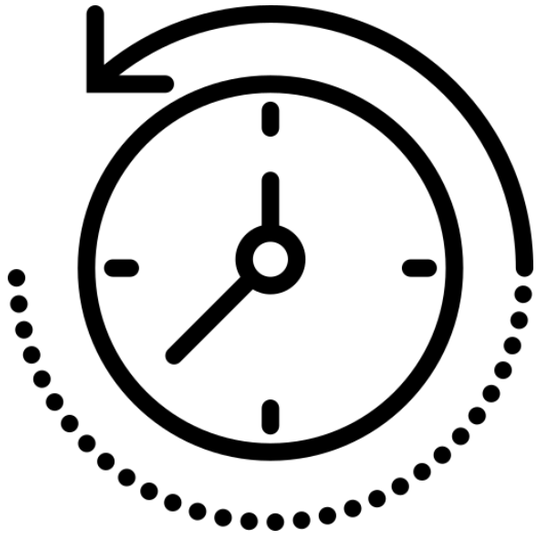
The Legal Basis for Pre-Transaction Monitoring

- Regulation 15(4) of the PMLFTR stipulates that if Subject Persons have knowledge or suspicion that a transaction is linked to proceeds of criminal activity or the funding of terrorism, they must refrain from carrying it out until they have informed the FIAU
- To effectively fulfil this obligation, a level of real time monitoring needs to take place.

Pre-Transaction Monitoring

When should Pre-Transaction Monitoring Checks be Completed?

- Traditionally, pre-transaction monitoring has been applied in situations where there is face-to-face contact.
- While Subject Persons are not expected to review every customer transaction, real time monitoring should be undertaken before processing transactions deemed to present a higher level of risk or involving higher risk customers.



Pre-Transaction Monitoring

High Risk Scenarios that Necessitate Pre-Transaction Monitoring

- Transactions linked to sanctioned individuals, entities, or countries
- Transactions involving individuals or entities with adverse media
- Transactions or behaviour indicative of certain predicate offences
- Transactions to/from high risk or non-reputable jurisdictions
- Transactions or activities inconsistent with the customer’s profile
- Transactions that diverge from the expected transactional pattern
- Unusually high value or anomalous transactions

Pre-Transaction Monitoring

Examples of Pre-Transaction Monitoring Checks

Obtaining an understanding of the background and purpose of the transaction

Engaging customers and requesting supporting documentation

Acquiring management approval for higher risk customers or transactions

List Screening

- List screening should not be the sole focus of pre-transaction monitoring.
- While screening against sanction lists, adverse media lists, PEP lists, and other watchlists is crucial, it is equally important to consider other factors such as the transaction type, transaction amount, and involved parties.

Pre-Transaction Monitoring Detection Rules

a.) Threshold-Based Alerts

- Transactions are alerted if an incoming or outgoing payment exceeds certain monetary or non-monetary thresholds.
- Implementation of daily, weekly and/or monthly limits for specific customers.

b.) Keyword-Based Alerts

- Alerts are generated if the transactions details or payment fields contain specific words that are of a more suspicious nature.

Pre-Transaction Monitoring Detection Rules

c.) Whitelisting and Blacklisting

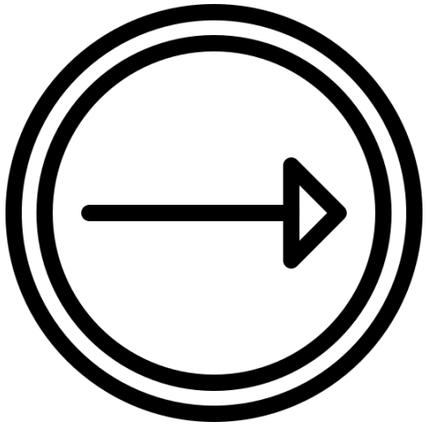
- Tailored limits can be set for certain established relationships between the customers and other third parties. These relationships can also be whitelisted by applying thresholds and parameters that are higher than normal. Likewise, payments to/from certain individuals or entities that fall outside of the risk appetite can be backlisted.

d.) Cash-Related Transactions

- Stricter detection rules can also be implemented to transactions that have a cash element and thus carry a higher inherent risk.

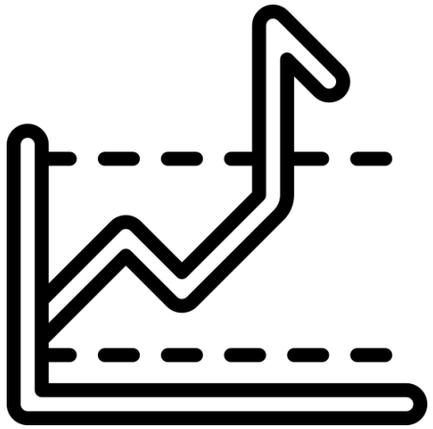
What is Post-Transaction Monitoring?

- Monitoring activities that are conducted after the transaction has already been executed, i.e., after the event.
- Post-transaction monitoring involves the holistic analysis of customers' transactions over a period of time.
- This type of monitoring empowers Subject Persons to detect trends, anomalies, and deviations that may not be evident from a single transaction but are significant when viewed in the context of the customer's transaction history.



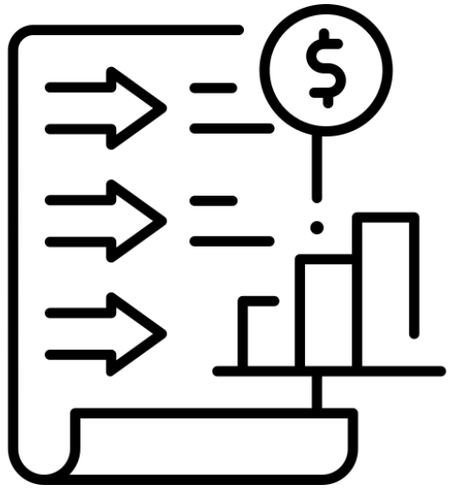
Customer Deposit Spikes

- When spikes in customer deposits are identified, Subject Persons should determine the purpose of the transactions and source of the incoming funds, as well as ensure that there exists a justifiable reason for these transactions.
- Any transactions that give rise to suspicion of ML/FT need to be reported to the FIAU without undue delay.
- If a red flag or trigger event is detected, it is crucial for Subject Persons to investigate the matter and take the necessary actions.



Post-Transaction Monitoring Reports

- As part of the post-transaction monitoring process, Subject Person can choose to generate post-transaction monitoring reports at pre-determined frequencies.
- Each report contains transactions of a similar nature that are grouped and examined together depending on the nature of the transactions and customer segments involved.
- Having access to wide range of post-transaction monitoring reports allows for a more holistic view of the customers' transactional patterns and overall activity.

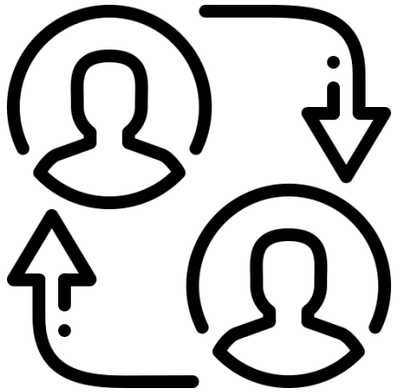


Post-Transaction Monitoring Reports (cont.)

 Cash Deposits	 Frequent and Small Transactions	 Structured Large Transactions	 Wire Transfers
 Monetary Instruments	 Account Turnover	 Peer Group Activity	 New Account Activity

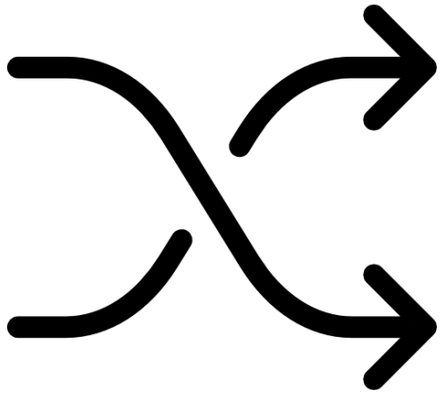
Peer Group Analysis

- This approach involves dividing the customer portfolio into homogenous peer groups comprising of customers with the same characteristics and risk ratings.
- Through data analysis, Subject Persons can compare the actual transactions and behaviour of individual customers to the average or expected transactional patterns of their respective peer groups.
- Any statistically significant deviations or outliers trigger an alert for further assessment.
- The effective comparison of peer group information is reliant on having a sufficiently wide customer base.



Optimal Mix – Integration of Both Pre- and Post-Transaction Monitoring

- The effectiveness of Subject Persons' transaction monitoring systems can be enhanced by incorporating elements of both pre- and post-transaction monitoring.
- Insights derived from carrying out post-transaction monitoring, such as transactional patterns, customer behaviour, and trends, can be used to continuously refine the set of initially configured detection rules applied as part of pre-transaction monitoring.
- Correspondingly, having a robust pre-transaction monitoring system in place means that the majority of unusual or suspicious transactions are identified and reviewed before they are executed.

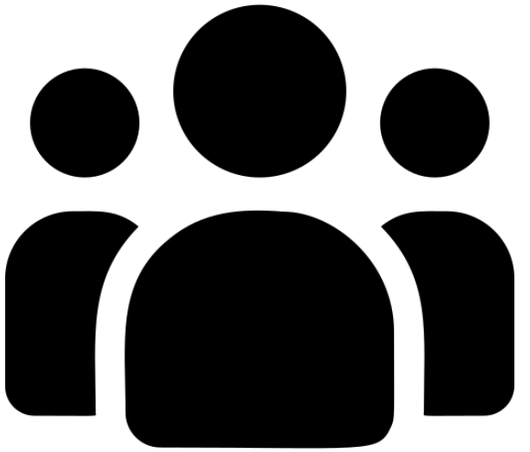


Detection Rules - Categorisations

Detection Rule - Customer

Factors to consider when configuring Detection Rules

- The Type of Customer (i.e. personal or corporate customer)
- The Customer Segment
- The Customer’s Size and Set-up
- The Customer’s industry
- The Customer’s risk profile and rating
- Duration of Customer relationship with Subject Person
- Comparisons with the customer’s age group



Risk Scenarios that can be applied

- Customer operating within a high-risk industry/sector
- Adverse media found on customer
- Change in customer risk classification
- Customer behaviour:
  - Monitoring the customer’s monthly/quarterly/yearly activity and comparing it to the same customer’s activity in the previous period.
  - Significant activity by new customer.
  - Significant deviations from past customer activity.
- Manual submission of a payment order
- Periodic customer profile monitoring – generates an alert if the review period has expired.

Detection Rule – Product/Service and Client Interface

Factors to consider when configuring Detection Rules

The specific products or services being offered by the SP such as banking, trade finance, wealth management, payment services and foreign exchange

Products/services that are more susceptible to being exploited for ML/FT purposes and/or fraud

The distribution channels (i.e. face-to-face or non-face-to face)

Risk Scenarios that can be applied

- Change in customer activity by product
- Cash withdrawn from unusual product
- Anomalous activities involving the use of bank cards (e.g. ATMs, credit cards or debit cards)
- Multiple deposits made by the same customer in different bank branches
- Over-pricing/under-pricing of products offered by customers
- Seasonal products being traded out of season or products sold outside their usual geographical market
- Payments by third parties unrelated to the customer for certain products that are not customary to receive payments from third parties, e.g. fixed deposit accounts, loan accounts and brokerage accounts

Detection Rule – Jurisdiction

Factors to consider when configuring Detection Rules

- The jurisdiction(s) where the customer or its beneficial owner(s) are based, have their main place of business or where the activity generating their wealth is carried out
- The jurisdiction(s) with which the customer has strong trading or financial connections
- The jurisdiction(s) with which the customer or its beneficial owner(s) have relevant personal links, e.g. the individual's residence in a given jurisdiction
- The anticipated or actual jurisdictional connections
- Whether the customer has any links to high risk, sanctioned or blacklisted countries
- The transactions' country of origin or destination

Risk Scenarios that can be applied

- Domestic vs international transfers
- Transaction activities with nexus to higher risk geographies
- Transactions to/from sanctioned or blacklisted countries
- Transactions to/from high risk jurisdictions with which the customer did not have any business dealings before

Detection Rule – Transaction

Risk Scenarios that can be applied (1)

- Aggregated cash/non-cash transactions
- SEPA vs SWIFT transfers
- Unusual patterns of cash deposits or withdrawals which may be indicative of potential structuring/smurfing, including aggregated frequent and small transactions
- Transactions that exceed a specified threshold that varies depending on the particular segment the customer falls in
- Rapid movement of funds in and out of a customer account
- Anticipated level and volume of transactions declared at onboarding not in line with actual activity
- Actual customer turnover exceeds the declared turnover in terms of transaction value or volume

Risk Scenarios that can be applied (2)

- High activity after period of low activity.
- High activity without any previous activity
- Aggregated amounts just below the threshold
- Credit followed by a debit (e.g. pass-through transactions) – compares a customer's incoming and outgoing payment activity to flag any unusual pass-through behaviour
- Transactions to/from legal arrangements such as estate management trusts and private foundations
- Transactions to/from high-risk industries/sectors
- Transactions to/from higher risk customers such as PEPs

Risk Scenarios that can be applied (3)

- Transactions in round amounts.
- Inter-company/group transactions – transactions between companies with a shared relationship/economic connection.
- Circular payment flows between originator and beneficiary – multiple transfers to/from the same counterparty.
- Customer account being used for different purposes, e.g. an account created to collect condominium payments being used for personal use
- Hidden and significant commercial relationships between customers evident through funds flows.
- Activities or behaviours consistent with certain predicate offences such as fraud, possible tax evasion or avoidance, corruption nexus, or funding of terrorism.
- Multiple reversals linked to particular customers.

Risk Scenarios that can be applied (4)

- Idle account with sudden activity
- Premature repayment of a loan
- Sudden emptying of customer account
- Substantial percentage of the available balance of the customer’s account used within a day
- Early closure of customer account
- Customer with frozen accounts affecting transactions through other non-frozen accounts
- Violations linked with the Fund Transfer Regulation