Table of Contents

Fraud Overview

As part of the Mojaloop ecosystem it is necessary to have a solution in place to ensure the system has the right level of monitoring and hooks in place to prevent fraud within the system. Fraud is one of the largest causes of revenue loss for service providers and financial institutions. It is critical that Mojaloop provides the infrastructure to allow for the real-time screening of transaction activity across users, accounts, processes and channels, to identify and prevent internal and external fraud in an organization.

The actual financial transaction is actually the last step confirming that fraud has taken place on the system, typically fraud happens very early on and the Mojaloop platform seeks monitor and identify fraud earlier in the process. By detecting fraud early in the process through proactive monitoring we can better protect the reputation, resources and revenues of those participating in the Mojaloop platform and ecosystem.

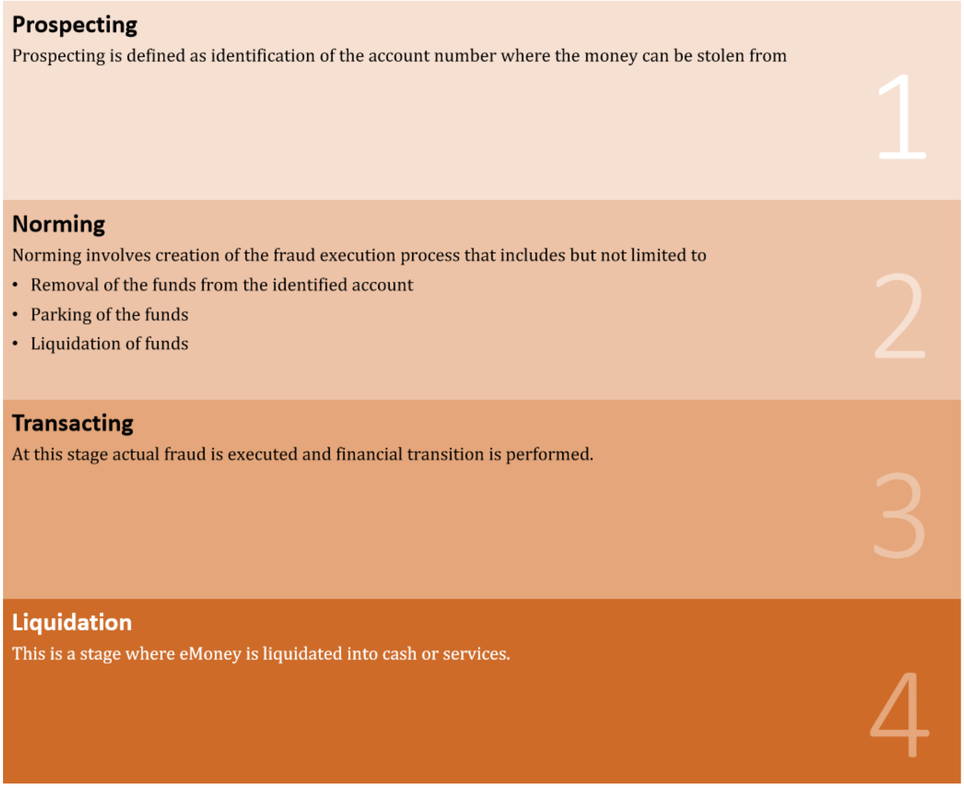
((Might have a simple diagram here to show how the fraud mgmt. system plugs into the Mojaloop hub; very conceptual))

Monitoring within the platform

The Mojaloop platform is not directly connected to the origination of the transaction, and will not have visibility of all the transactions flowing through a DFSP. Solution to address Fraud or Money laundering will be developed to ensure that it is able to detect fraud when there is only partial data.
For future enhancements extra meta-data could be provided by the DFSP, however that has not been factored at this stage.

Without end to end visibility of all the business flows, the system will be able to assist in the identification and tracking of fraudulent activity – and will have differing levels of success in identification of the key fraud typologies in Mobile Money Creation; E-Money Movement Fraud; E-Money to Cash Fraud; Profile Management / Account Management Fraud; Integration Fraud; Syndicate Fraud.

Financial transactions or cash out are the last opportunities to stop fraud and recuperate any money that might have been lost. To address any issues before this final stage, we have identified 4 stages of potential fraud where monitoring can be used to intercept issues:



Prospecting

Prospecting is defined as identification of the account number where the money can be stolen from

1

Norming

Norming involves creation of the fraud execution process that includes but not limited to

- Removal of the funds from the identified account
- Parking of the funds
- Liquidation of funds

2

Transacting

At this stage actual fraud is executed and financial transition is performed.

3

Liquidation

This is a stage where eMoney is liquidated into cash or services.

4

There are 2 main types of suspicious transaction that the system must be able to identify

- Transactions that were manipulated (i.e. Employee or Man in the Middle)
- Transactions that show suspicious behaviour – i.e. a known pattern of behaviour, or an abnormal pattern for a specific entity

Once suspicious activity is identified the service will allow the tracking of a case through to its conclusion. With options for statutory reporting, as well as case management overviews. Case management will need to ensure that incidents identified by DFSPs can be captured, and activity aligned, and any incidents can be notified to the DFSPs

Identifying Suspicious Transactions

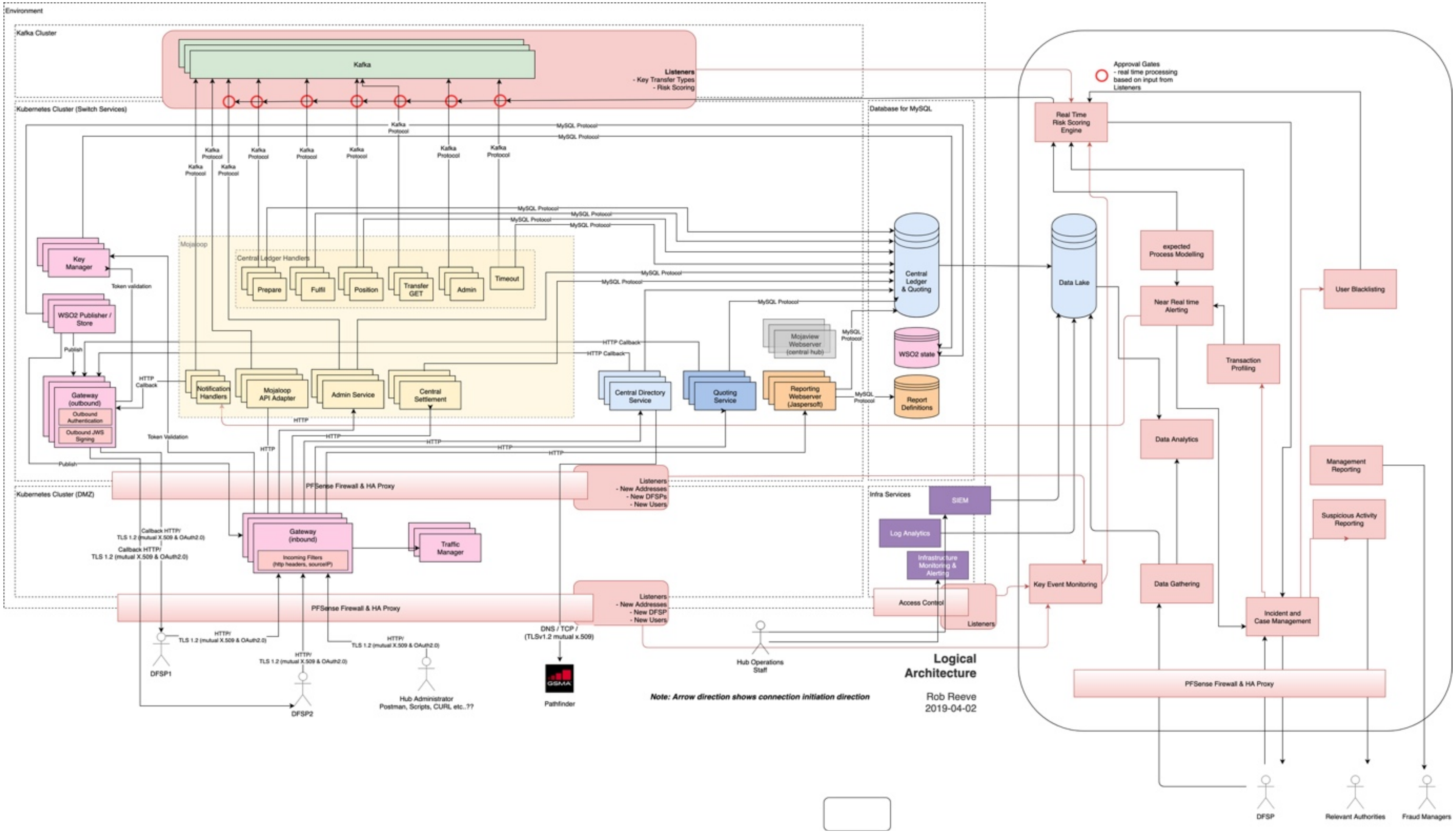
- Map standard and expected activity and alert if abnormal behaviour seen
- Map and monitor key events that could be warnings of a compromised system and therefore increasing the risk profile of transactions
  - Change in a DFSPs Certificates or IP address
- Provide user profiles of behaviour– both healthy and suspicious
  - User level
  - DFSP level
- Provide analytics and reporting to create new profiles, that can then be applied to the monitoring tool
- An assessment of an incident creates feedback to a fraud Typology to improve detection and reduce false positives

- Assign a default profile type based on data provided by a DFSP
- Detect change in behaviour (from profiling)
- Provide AML risk scoring of a transaction
- Default actions based on risk score
    - Proceed
    - Alert
    - Block
- Change initial AML risk rating automatically depending on user or DFSP actual behaviour.
- AML provided in near real time
- CTF is considered out of scope, as the full user data may not be available – this task MUST reside with the DFSP.

Managing Incidents and Alerts

- Configurable case management workflow process
- Consolidation of incidents with similar attributes into single case
- Removal of incidents that are later identified to be different
- can regroup alerts to form cases according to certain rules
- Ability to minimize false positives
- system able to tailor recipient of alerts depending on profiles.
- monitor how long cases remain pending
- Alarms if items are not reviewed in configurable timeframe based on queue type and invoke an escalation request
- propose different queues per type of incident (for example, internal fraud)
- Provide a Workflow to interact with DFSPs or Law Enforcement Agencies
    - DFSP notification of suspicious activity initiated from within the platform or by the DFSP
    - Law enforcement liaison -allowing access to limited data, pertaining only to that case, with all tracking and approval
    - SAR submission

Integration with existing Mojaloop Systems



Logical Architecture

Note: Arrow direction shows connection initiation direction

Rob Reeve
2019-04-02

Detailed Requirements

AML / Fraud

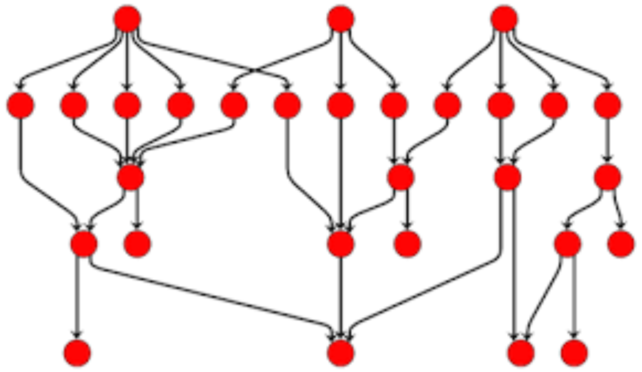
Business Overview

The introduction of real time transfer amongst multiple entities, the opportunity for funds to be moved quickly amongst different DFSP accounts rapidly increases. By introducing the ability to track funds movement, the hub can quickly identify all suspicious actors within the ecosystem, ensuring that all DFSPs are notified of the impacted accounts, and that any funds remaining can be ringfenced – and potentially returned to the original party.

In addition to the monitoring of externally initiated transfers, by creating a map of the normal behaviour of transfers, and management of key events, the potential for internal fraud is also reduced or quickly identified

Requirements

- Create a standard pattern of transactional data – mapping of all the steps in a transfer
- Identifying abnormal activity and raising a corresponding incident in the case management platform
    - Abnormal pattern
    - Anomaly from Logs
- Add new flows as they are created in the Switch
- Add and monitor key events – which could signify a compromise to the integrity of the platform
- Create a visualisation of actual Money flows, so that a suspicious transaction can be followed and additional connected accounts quickly identified - Allowing for the request and import of additional data from DFSPs



- Graphic representation of links / transactions between parties ("Heat Map"). Reporting XX volume / Y transactions / in period z
- The visualization (link analysis) parametrized per analyst – i.e. different roles have different levels of information

- Visualization (link analysis): different colours reflecting various level of risks + thickness of lines reflecting volumes of transactions (subject to currency)
- Customized profiling to support querying of underlying data, i.e. detection on any abnormal / deviation of transactional behaviour on configurable portfolios of entities or individual entities
  - Merchant/partner based analysis:
  - Average transaction value, ranges, deviation analysis;
  - Transactions outside working hours for classified organisations such as merchants;
- Alerting of rapid movement of funds after deposit
- Ability to use any of the above to create an incident for capture into the appropriate queue in the case management system.
- Continuous monitoring and alerting of all transactions
- Detect change in behaviour (profiling)
- real time user blocking
- User communication
- DFSP Communication

Real time Transaction Monitoring

Business Overview

Although certain activity might be clearly identified as Fraud or Money Laundering, some transactions are not as clear to identify. To support in identifying new cases of fraud or suspicious activity, risk scoring is implemented to help prioritise investigations and assist in removing false positives. Using information, where available, to augment the transaction data with incremental data that can assist in the identification of higher risk activity.

Incremental information may come from the DFSPs so the system will have the option to automatically accept it. Alternatively the system will reach out to request the Data from the DFSP and import it, if the information is required as part of an investigation.

Once a transaction has been scored, if it is too high a risk, then it will be flagged immediately, either for approval by the DFSP, or by the Switch Operator. There will be a default time set in which a decision must be made, and either the transaction will be rejected or accepted automatically. In either case, the transaction will be recorded in the case management service to ensure that learnings from the decisioning and transaction can lead to improve automated responses.

Risk Scoring

- based on national / international services
- based on currency
- scoring amended based on different DFSPs
- Region (where the DFSP is based),

- location of payment origin
- location of payment destination;

Possibility for DFSPs to add

- IP address
- Geo-location data – both GPS and Radio data
- Detection of 2 subsequent transactions that could not be executed by a single individual in different places (integrating flights timings, etc…)

Risk scores should be assigned by:

- Transactions outside working hours for shops;
- Transaction Velocity (Number of transactions per hour/day/week/month) per account
- Transaction Value (Individual/cumulative – combined by hour/week/day/month) per account
- Transaction Velocity (Number of transactions per hour/day/week/month) per customer
- Transaction Value (Individual/cumulative – combined by hour/week/day/month) per customer

Transaction Authorisation

- authorise, suspend or reject transaction notifications on the mojaloop platform;
    - a rejected transaction will create an incident in the case management module – with appropriate reasoning.
    - An approved transaction will be logged
- Flag a transaction for further validation i.e. the transaction is neither rejected or authorised, it instead requires additional validation through manual processes;
    - The flag will be sent to the DFSPs platform where the transaction will be suspended with the case management module setting the appropriate flag of authorise or reject transaction once the case investigation is concluded;
- Data processing for scoring of real time transactions should not negatively influence on customer / end user experience. With a transaction approval being concluded in under 400ms.

Near real time Pattern Analysis

Business Overview

Some fraud is immediately identifiable, other activity may require more transactions before the true intent of the perpetrator becomes obvious. Additionally the overhead of multiple transactions being analysed can lead to a situation where legitimate transactions are delayed. To overcome these challenge, a near realtime solution is required. This allows for different analyses to be prioritised – i.e. high value or high volumes so although the original transfer might not be stopped, any fraudulent transfers might still be identified in time to allow the recovery of the funds.

Any activity that is identified as suspicious can be added to the default transaction profiles, to support further assessments. Reducing the time to find suspicious transactions, but also supporting the reduction of false positives.

Where possible, the activity of users can be used to create healthy and unhealthy profiles – any deviation from the norm can be used to identify suspicious actors, or create a more robust profile and less false positives.

Transaction Analysis

Analysis of the various transactions

- Currency used for the transaction i.e. international payments
- a short period analysis of set rules (i.e once in every 4-6 hours - exact time to configurable).
- Validation of transactions over a defined period of time (i.e. day, week, month):
  - accumulated amount per single sending or receiving actor
  - accumulated volume per single sending or receiving actor
  - total number of transfers to different DFSPs
- transactions that have been performed at certain time, i.e. over midnight – to bypass controls
- Cumulative analysis of all outgoing and incoming transactions associated with single customer over a period of time.
- Violation of set rules trigger an alarm and opening of an incident.
- Automatic blacklisting of detected customers
- Association analysis of internal user and DFSP during limited time period.
- Test transactions.
- Transactions outside working hours.

Any patterns can be used to create a new risk type with New Indicators / Profiles

Actor Analysis

Analysis of the various actors, and the ability to perform the following analysis.

- be able to raise early warning alerts based on peer pattern analysis – deviation from a predefined profile, where historic transactions which did not flag, can be used to assess the risk of a repeated incident, and increasing the risk score of transactions
- Deeper Customer analysis
  - Behavioural scoring based on transactions type, amount, frequency, destination;
  - Analysis of transactions by customer groups
  - Reversals requests by frequency, or type of transaction;
  - Average transaction value, ranges, deviation analysis;
- Customer Usage profiling, and the addition of supplementary data feeds and risk scores

- Actor Location
- Actor age (where known)
- Length of relationship with Actor (where known) = time with DFSP
- Violation of set rules should trigger an alarm and opening of an incident.
- Automatic blacklisting of detected customer should also be configurable.

Any patterns can be used to create a new risk type with New Indicators / Profiles

Case Management

Business Overview

Once any suspicious activity is identified or a real time alert is raised, the ability to manage the assessment and communicate with other actors in a real time manner will lead to an improved user experience in the case of false positives, and an improved chance of recovering funds in the case of suspicious transfers.

As an emergency response to the case management system being unavailable, the system can be configured to restrict certain transaction types by default. Such an approach being adopted to prevent high risk transactions being approved inadvertently.

The ability to share sensitive information in a controlled way is also critical. The incorrect processing of an incident can lead to an end user inadvertently becoming blocked, or in the worst case scenario, blacklisted from transacting.

Incident creation and alerting

- Every transaction rejection or suspension notification is a trigger to create an alarm and subsequently open an incident in the case management module;
- The systems may have further feedback from the MFS platform regarding the success of a requested transaction. I e cases where the platform sends a reject or suspend notification, but MFS still proceeds with the transaction, this should be regarded as an incident and is a trigger to create an alarm and subsequently open an incident in the case management module; and
- ability to detect deviation between expected behaviour and actual behaviour
- Detection and analysis of abnormal activity based on individual scoring;

In case the AML real time monitoring module is not available (not replying), the switch should automatically discard all transaction requests. A special type of alarm will also be configured for such cases with automated registration of downtime start and finish. This downtime should correspond to the recorded platform down time.

Case Management

- Configurable case management workflow process
- Consolidation of incidents with similar attributes into single case
- can regroup alerts to form cases according to certain rules
- Ability to minimize false positives

- system able to tailor recipient of alerts depending on profiles.
- monitor how long cases remain pending
- Alarming if items are not reviewed in configurable timeframe based on queue type and invoke an escalation request
- different queues per type of incident
- Provide a Workflow to interact with DFSPs
- Provide a Workflow to interact with Law Enforcement Agencies
    - Law enforcement liaison -allowing access to limited data, pertaining only to that case, with all tracking and approvals

- All incidents should be stored in the case management module for X months
- Each incident should be assigned an automatically generated unique ID. It should not be possible to delete or change incident records.
- A GUI allowing a user to filter, sort, aggregate or drill down incidents and escalate them.
- configurable access levels and related rights. There should be the possibility to show partly encrypted data for certain level users (I e only 4 digits for bank card etc)
- configurable incident types, status, severity levels, deadlines for incidents closure.
- manage certain rules in the real time transaction monitoring module and subsequent transactional feeds. I e incident of partial coincidence of KYC data with sanctions list could be resolved as positive and “discard transactions” rule should be applied as case resolution.
- integrated with reporting module.
- notify different lists of employees by e-mail or SMS depending on incident severity.

User Blacklisting or Restricting

Business Overview

The ability to identify a suspicious actor and then add them to an increased risk profile, or even blacklisting prevents a rogue character from continuing to commit fraud or launder money, however it also exposes the service to challenges if it prevents an individual from transacting – i.e. unable to pay for basic necessities.

As such implementation of Blacklisting of users must be done with simple controls to reduce any blocks on that user. Access to the data being securely monitored and the use of maker/checker or Creator/Verifier/Authoriser level controls to ensure that proper diligence is provided

User Restriction Requirements

- Clear identification of users – to prevent incorrect classification
    - Names / Aliases
    - DoB
    - Address where known

- Process for Identifying type of restrictions
- Process for managing disputed identification or activity
- Process for securely transferring evidence and information to and from DFSPs, whilst tracking what information has been shared – so any subsequent reversal of a decision is shared with the same parties
- Ability to set profile restrictions based on DFSPs risk appetite
- Ability to share specific information with affected party/ies
- Multi-level authorisation for key decisions

Reporting

Business Overview

With the volume of information and possible number of incidents, management insight is fundamental as is the need to report to external agencies. The system needs to automate and simplify most of this task to ensure that resource is not spending time reporting, instead focussing their time on assessing the identified incidents.

Reporting Requirements

- a GUI with configurable dashboards and the ability to extract data (but also report on the extraction)
- Reports should represent data aggregated for DFSPs, internal users, alarms, number of incidents by status etc.
- The module should keep standard Suspicious Activity Report (SAR) forms for the relevant Country.
- The AML analyst should be able to generate a SAR from selected data, check the result and escalate to an AML officer of higher rank
- Rules based view of certain information and reports – restricting access privileges based on user profile

Platform configuration options available

- Ability to move activities between various monitoring states - real-time monitoring to near real time and offline
- Use and maintain a data base of AML schemes depending on industry – DFSP as Mobile Money Operator vs Bank
- System is able to auto-refine rules based on false positive rates ("machine learning")
- Access to information fully configurable per user's profile – where known
- Allows roles configuration per user and segregation of access depending on client portfolios (as example, per country)
- Separation of Fraud Profiles – critical / non-critical, additional categorisation or investigation routing and decision impacts in payment flows
- Sandbox functionality – to allow prototyping of profiles and rules, without impacting
- Unique ID per consumer ➔Mobile number or another ID, can all be merged to create a single view
- Separation of Apps Investigation / Admin functions

Connection to additional sources

(future functionality for hubs that have a central ID)
To ensure the analysis has the maximum amount of data, additional data sources should be available, as a minimum

- able to import data from external data base Such as DFSPs
- Integration with Dow Jones, Thomson Reuters etc., data bases
- system able to process alerts based on Keywords and scroll the internet - web crawling – i.e. brand risk management)
- Process internal black list
- Open Source Intelligence data sources
- Tools to manage conflicts in sources of information

Additional Requirements

Adhering to local data protection, biometric and card provider laws and requirements (such as PCI or GDPR) – with the ability to identify and protect sensitive data when it is stored.