



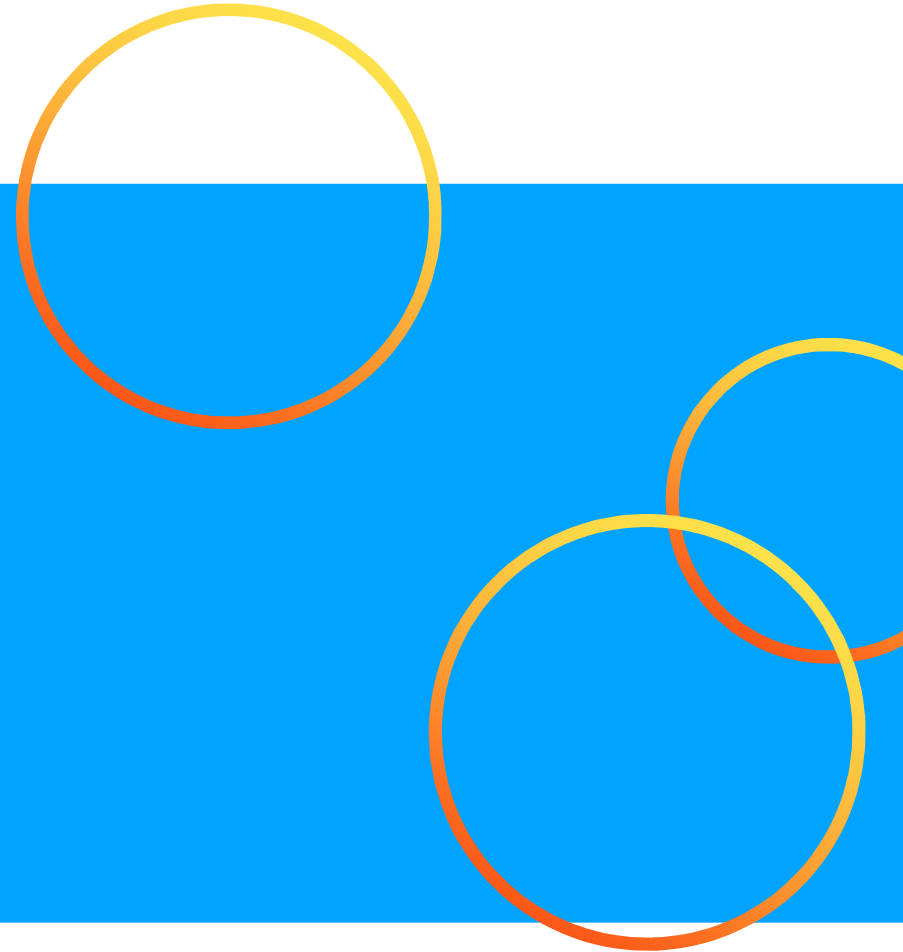
# Mojaloop Fraud Risk Management

Justus Ortlepp – Product Owner, LexTego

Rob Reeve – CEO, LexTego

Greg McCormick – Director, Sybrin

Jason Darmanovich – Architect, Sybrin



# AGENDA

---

- The Introduction
    - The journey
    - The Fraud Risk Management solution
  - The Proof of Concept
    - The concept
    - The integration architecture
    - The **Actio** architecture
    - The fraud risk typologies
    - The **APRICOT** model, part IV
    - The data factory
    - The demo presentation
  - The Next Steps
-

# The journey so far...

## PI 9

Fraud Risk was selected for further work “To review and classify the typologies to determine which of those strategically fit with Mojaloop’s vision and how to get started building it”.

- The development of a strategic assessment framework
- The detailed classification of the risk typologies already identified
- A detailed cross-reference between the risk typologies and the data dictionary already developed

## PI 10

Fraud Risk Management was selected as a work-stream for PI10 with the broad objectives to define, investigate and validate a backlog and MVP for a FRM system/service against the APRICOT modelling for existing/prospect operators; and identify partners to build / implement a FRM system / service.

Objectives for PI11 and beyond were identified and prioritized.

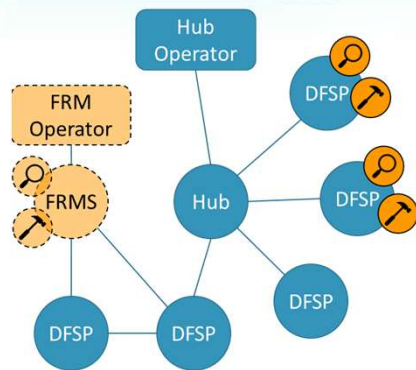
## PI 11

The Fraud Risk Management workstream had following tasks for this program increment:

- Identify the typologies that are visible to the hub and can be monitored by the hub
- Identify additional typologies related specifically to fraud “at the hub”
- Consider the feasibility of an Open Source Software Fraud Risk Management solution

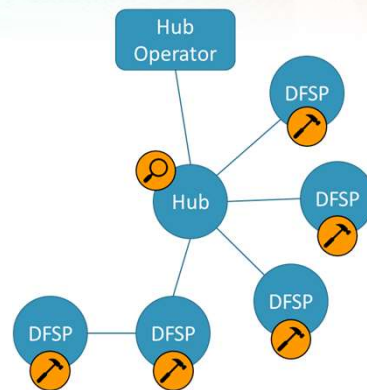
As a result 39 new typologies were identified. These typologies are core fraud risks that a hub faces and have to be mitigated at hub level.

# Operating model configurations



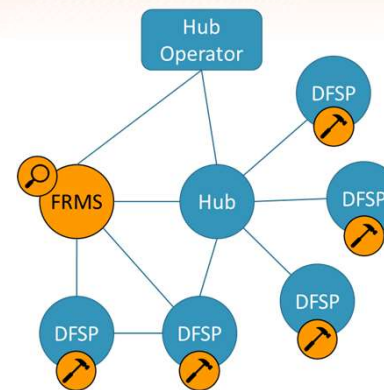
## Distributed

- No fraud risk detection or management capability or responsibility by the switch Operator
- Some FSPs perform detection on internal (on-us), incoming and outgoing transactions
- Those FSPs would employ compliance teams to investigate fraud and financial crime risk alerts



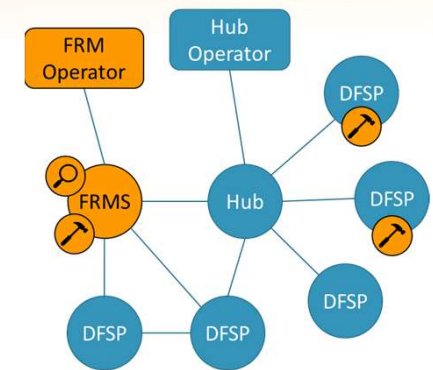
## Embedded

- Centralised fraud risk detection service hosted by the switch Operator
- The Operator performs detection on all transactions routed through the switch
- Each FSPs would employ compliance teams to investigate fraud and financial crime risk alerts issued by the Operator



## Semi-attached

- Centralised fraud risk detection service hosted by the switch Operator
- Separate interface to receive transactions from switch participants and non-participants
- The Operator performs detection on all transactions routed to the FRM service
- Each FSPs would employ compliance teams



## Standalone

- Autonomous and independent fraud risk detection and management service hosted by an FRM Operator
- Discrete fraud detection
- Outsourced fraud management
- The FRM Operator performs detection on all transactions routed to the FRM service
- Shared, centralised compliance services

# FRM: Programme Increment 12

Data interface

## FRM SYSTEM

Transaction monitoring

Blocklist management

Fraud risk detection

AML/CFT detection

Alert & Case management

Collection, transformation and enrichment of transactional data received from the switching hub

Evaluation of every transaction routed through the switching hub

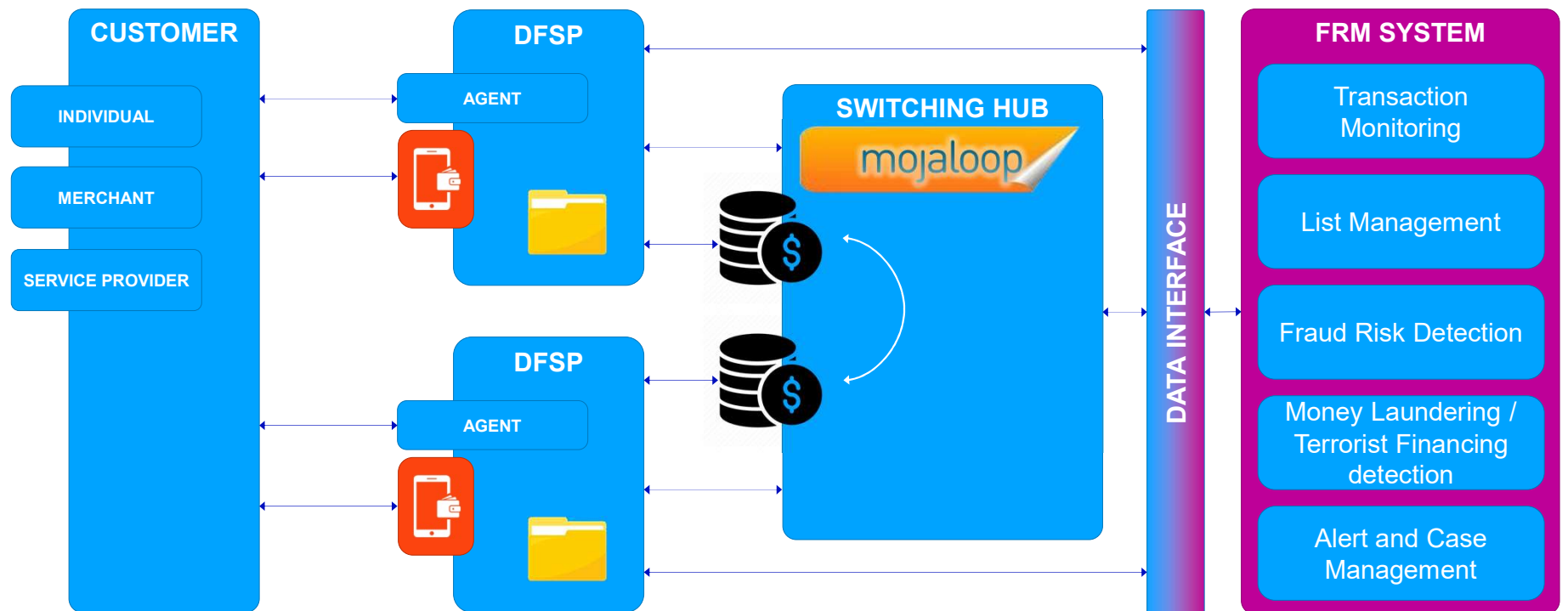
Realtime transaction routing based on the status of the transacting entity within the system

Realtime and near-realtime evaluation of an incoming transaction against selected fraud risk typologies

Near-realtime evaluation of an incoming transaction against selected money-laundering risk typologies

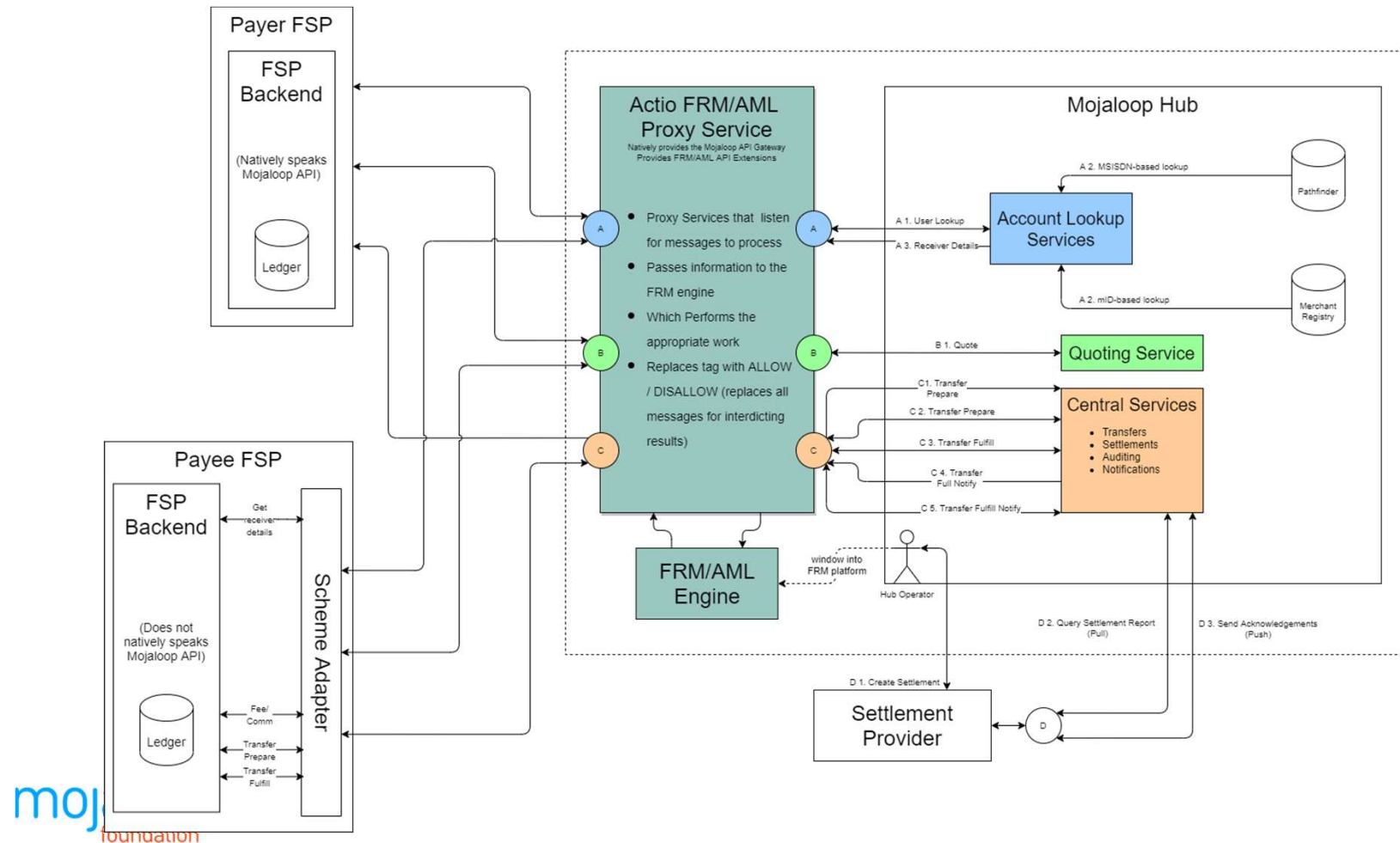
Distribution and investigation of alerts, along with the associated case management systems and workflow processes

# The context



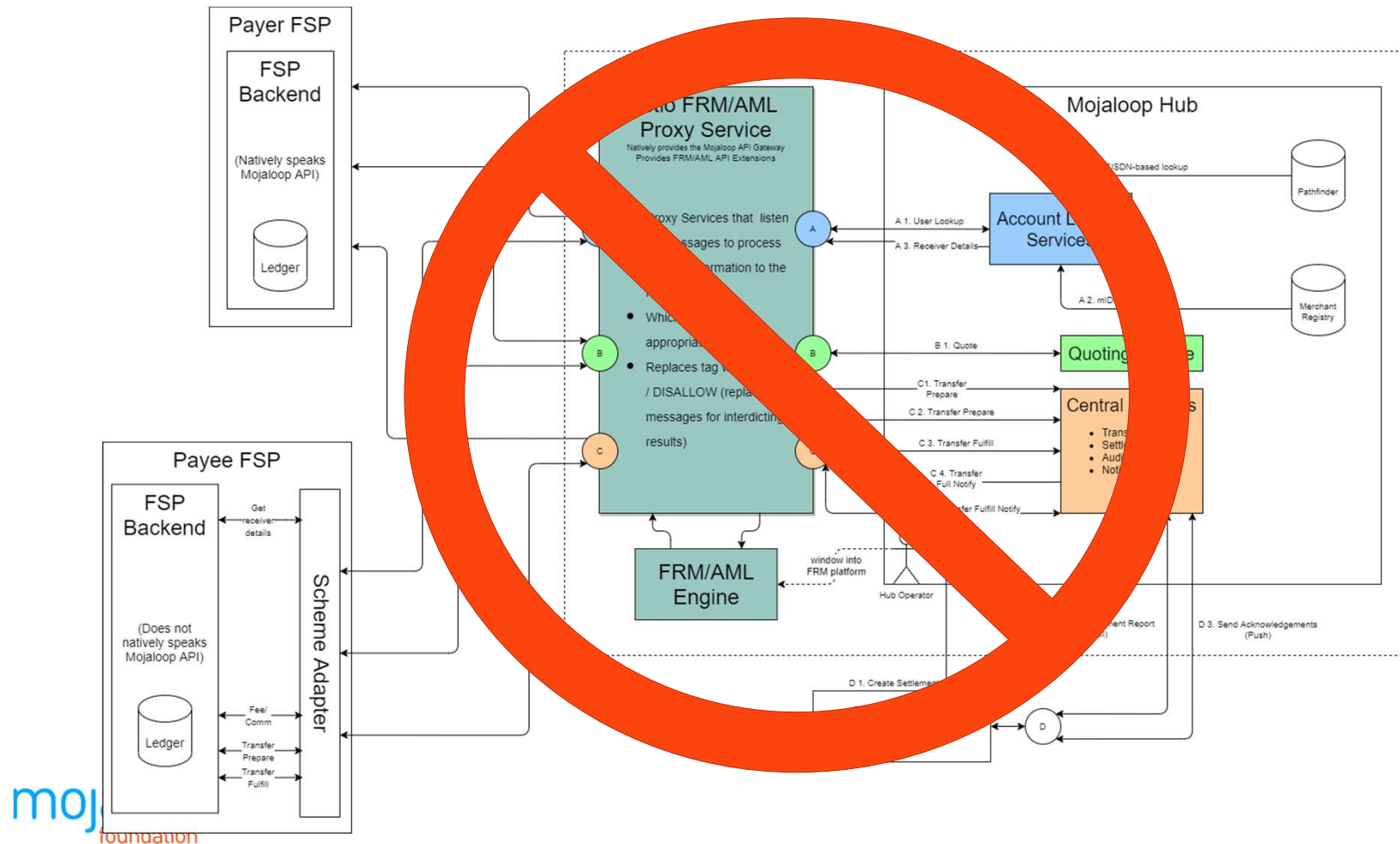
# ARCHITECTURE

# The integration architecture

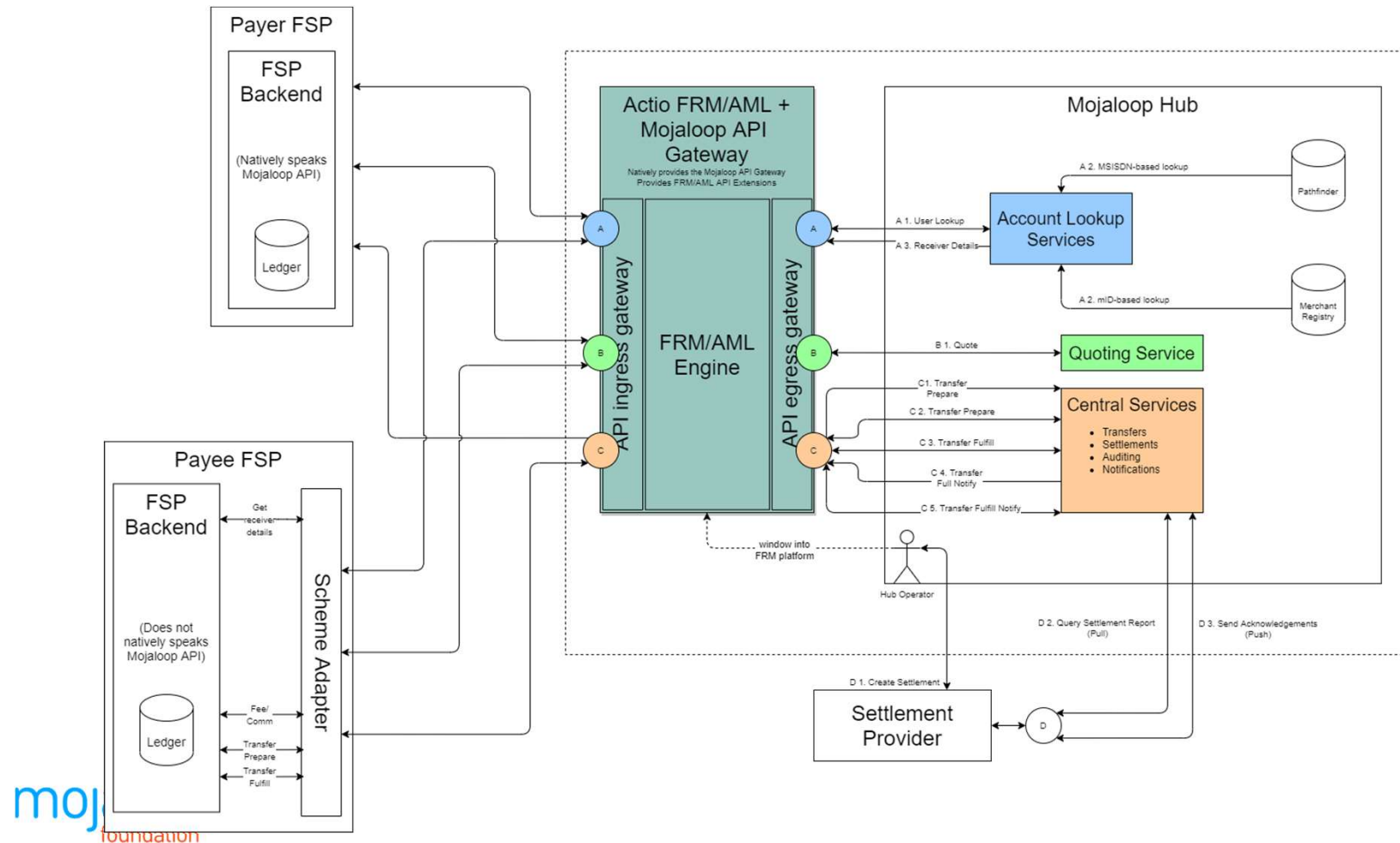




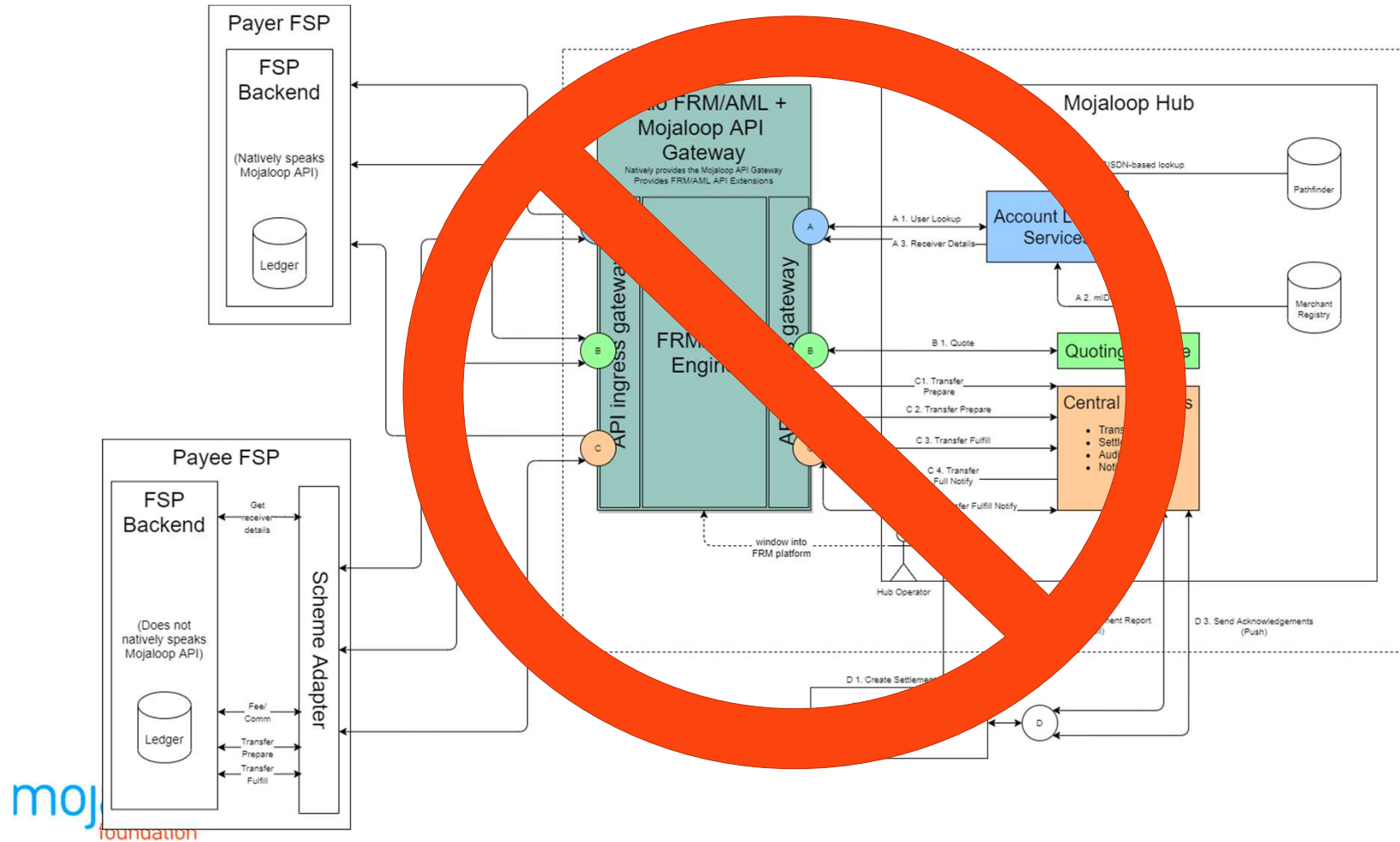
# The integration architecture



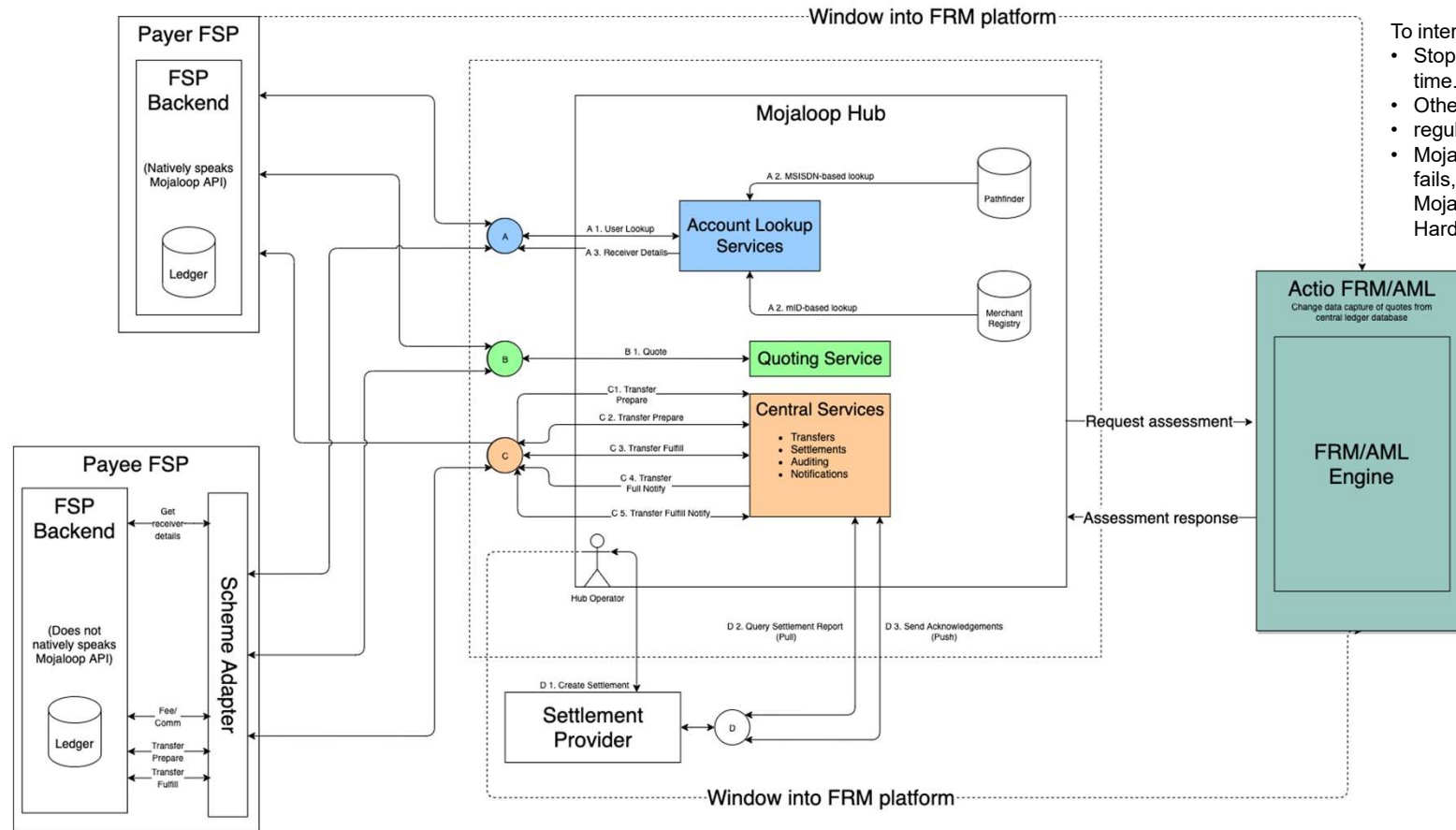
# The integration architecture



# The integration architecture



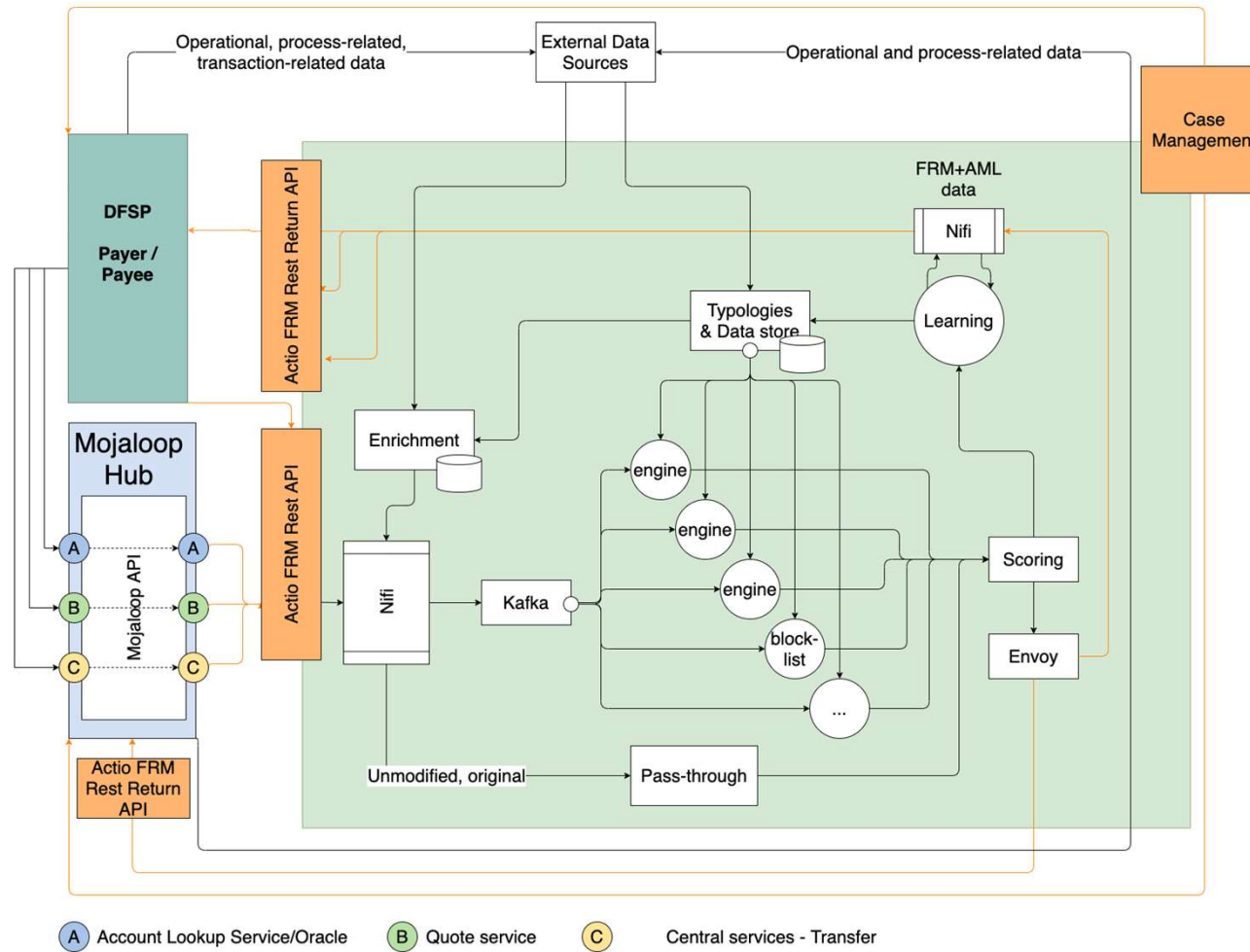
# The integration architecture



- To interdict or not?
- Stop a transaction in flight real time.
  - Other systems need it, regulators want it,
  - Mojaloop's model completes or fails, times out etc. For Mojaloop do you Interdict, Hard stop?

# The integration architecture

Interface Points in Orange



# The integration architecture comparison

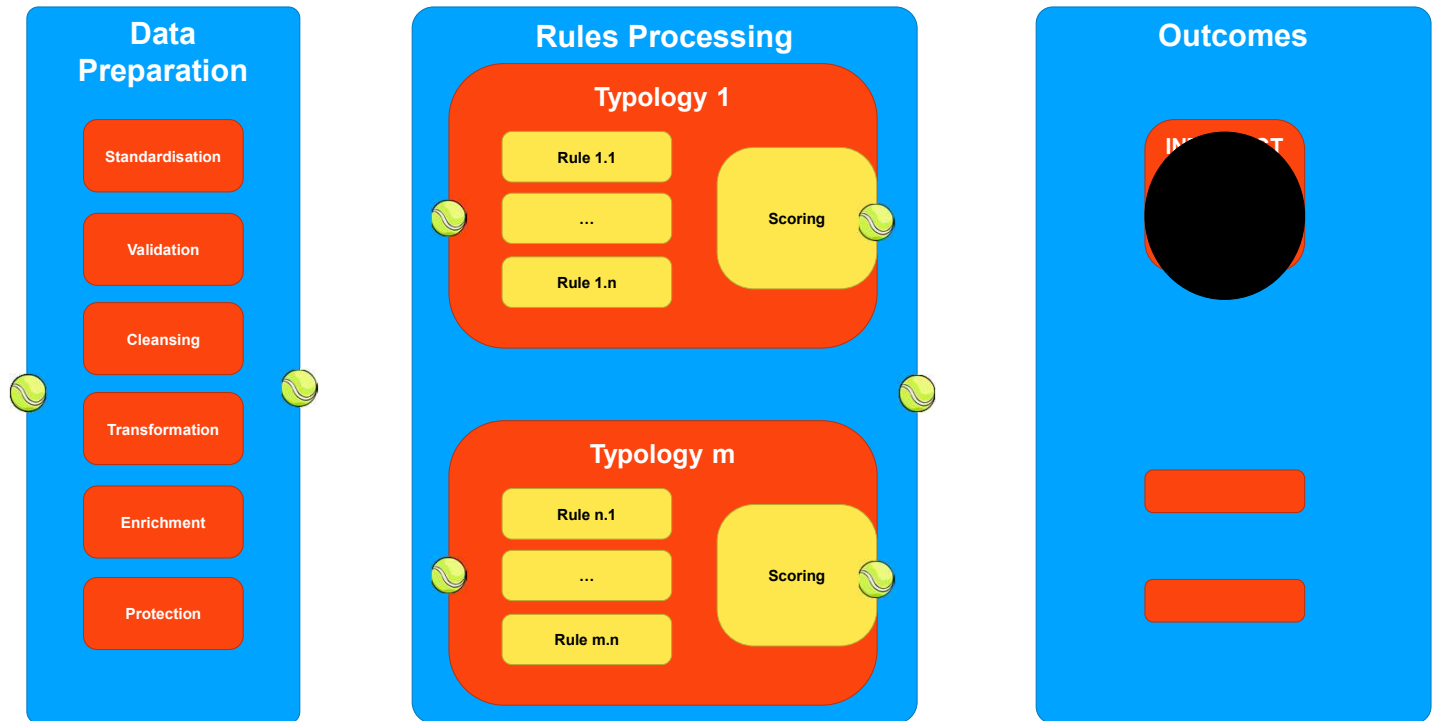
Proxy model	Gateway model	Streaming model	Service model
<ul style="list-style-type: none"> <li>+ Passive - minimal friction in implementation.</li> <li>+ FRM is no longer in critical path of transaction flow in Mojaloop.</li> <li>+ Does not require the implementation of a potential circuit breaker.</li> </ul>	<ul style="list-style-type: none"> <li>+ Drop-in replacement for existing component with no external functionality changes</li> <li>+ Can be implemented in a pure pass-through fashion so that the Mojaloop software can be installed without enabling the FRM solution, whilst still installing the FRM solution for later use</li> </ul>	<ul style="list-style-type: none"> <li>+ A relatively simple implementation approach as it requires minimal integration between ACTIO, DFSPs and Mojaloop.</li> <li>+ Ability to ingest all historical data</li> </ul>	<ul style="list-style-type: none"> <li>+ Decoupled, and works with any system via API</li> <li>+ Supports the previously agreed to preferred method of semi-detached.</li> <li>+ Can support interdiction</li> <li>+ Historical data passed to us and we subscribe to data sources via ETL methods.</li> </ul>
<ul style="list-style-type: none"> <li>- Effectively a man-in-the-middle attack architecture. Compromising the proxy would allow all transactions being handled by the Hub operator to be intercepted, changed, replayed or blocked.</li> <li>- Maintenance could be more difficult over time</li> <li>- Requires both Mojaloop and DFSPs to agree to use the proxy, which makes uptake more difficult and increases friction in the sales and implementation process.</li> </ul>	<ul style="list-style-type: none"> <li>- Potentially more complex to maintain the ACTIO FRM solution as a gateway</li> <li>- Requires providing alternative Helm charts for Mojaloop implementation</li> <li>- As with any gateway, if compromised could act as a man-in-the-middle attack vector.</li> </ul>	<ul style="list-style-type: none"> <li>- Does not allow for interdiction. The FRM solution therefore becomes a passive solution only generating information for potential follow-up.</li> <li>- Requires Hub operator to install additional software and potentially additional hardware within their implementation of Mojaloop, and configure the FRM solution appropriately.</li> </ul>	<ul style="list-style-type: none"> <li>- Requires DFSP to install additional software and potentially additional hardware within their implementation of Mojaloop, and configure the FRM solution appropriately.</li> <li>- Works best with a service provider or other central system of shared data.</li> </ul>

# The FRM concept

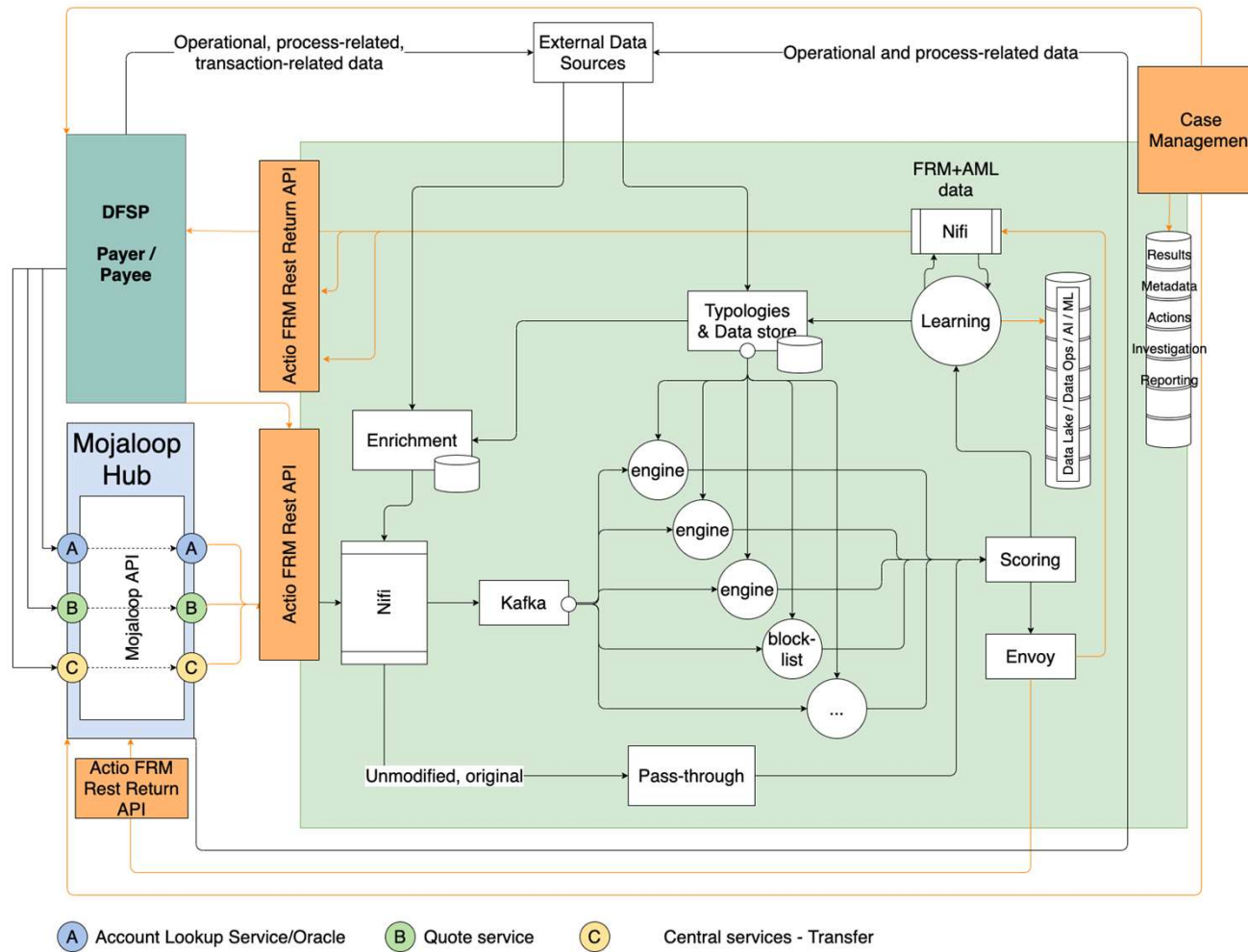
... the whole thing can be built in Open Source Software!



mojaloop  
foundation

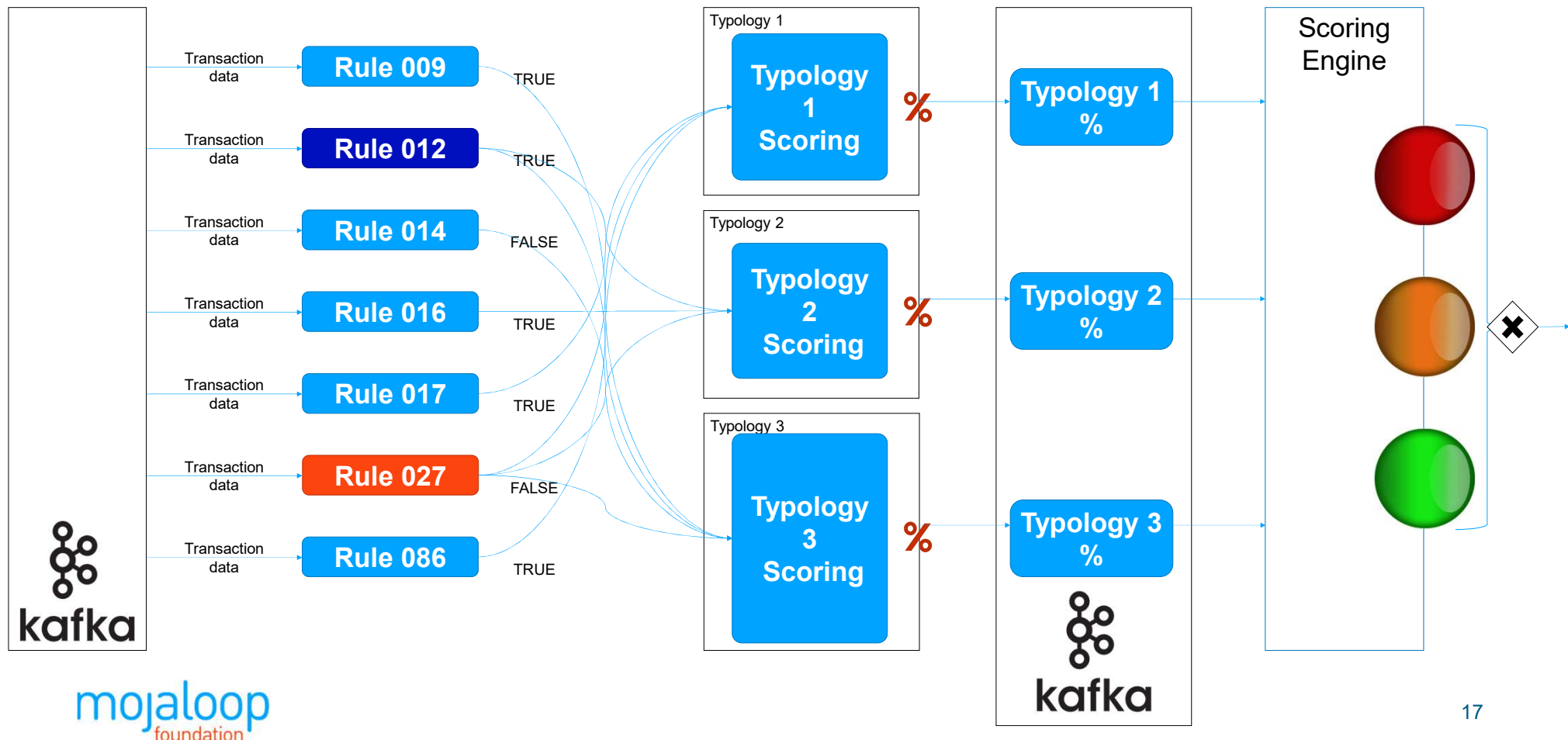


# The internal architecture

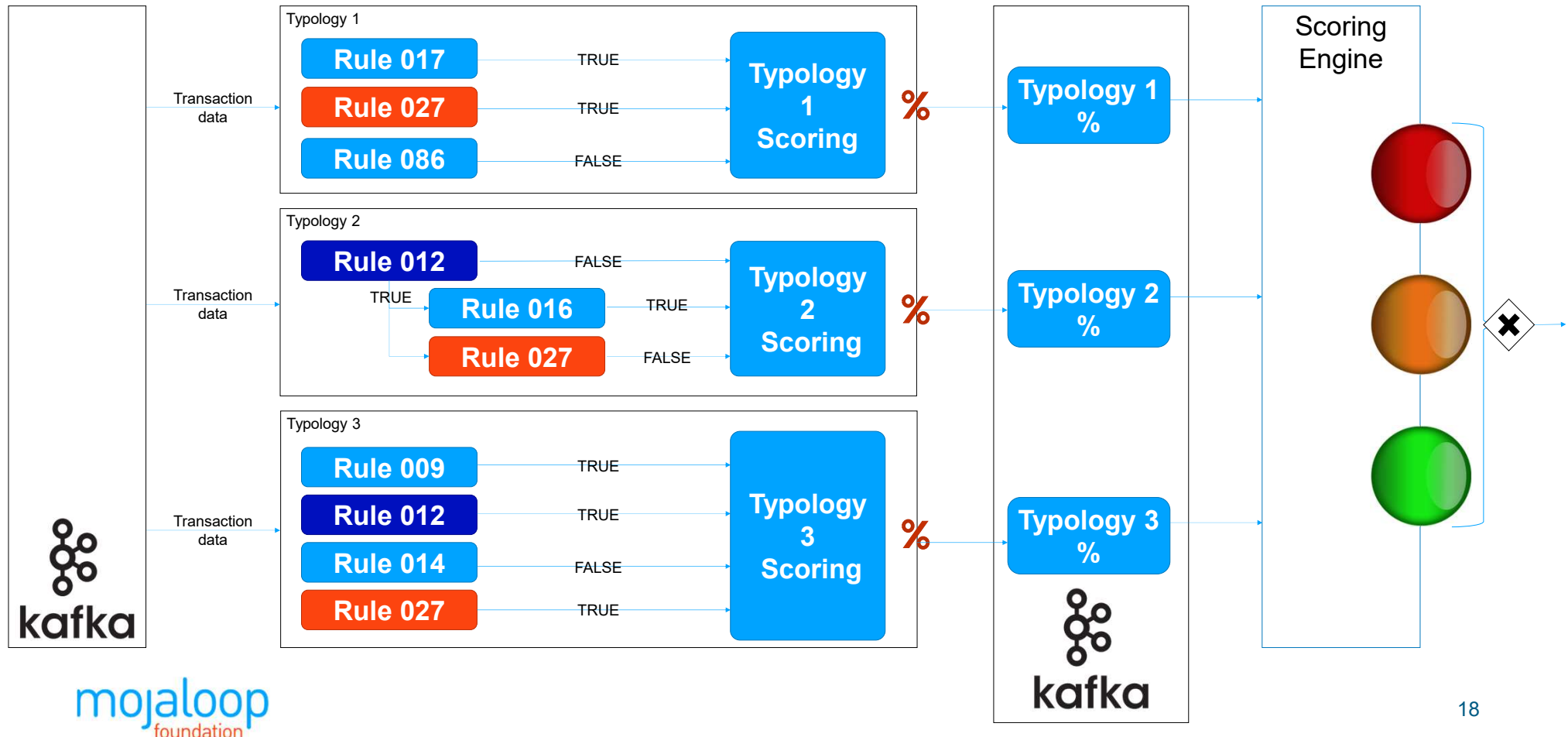




# The pipeline-based approach



# The typology-based approach



# The typology processing and scoring

- Two approaches for processing and scoring typologies were developed. The intent was to deliver one approach during the POC and complete the assessment or the other early in the MVP.

	<b>Pipeline-based approach</b> A design pattern used in large scale MQ ODM Systems	<b>Typology-based approach</b> Processing a complete typology as a microflow
<b>Upside:</b>	<ul style="list-style-type: none"><li>+ Each Rule Fires Once – Efficient</li><li>+ Normalized Structure Supports Maintainability</li></ul>	<ul style="list-style-type: none"><li>+ Easier to build</li><li>+ Denormalized, potential to be very fast</li><li>+ Less computational complexity</li><li>+ Easier individual rule parameterisation</li></ul>
<b>Downside:</b>	<ul style="list-style-type: none"><li>- Complex to Build</li><li>- Orchestration More Involved</li><li>- Complexity requires a design that can handle the threading and parallelism</li><li>- Rule parameterisation by typology results in rule duplication</li></ul>	<ul style="list-style-type: none"><li>- Runs process engine multiple times, once per typology that needs it</li><li>- At scale, additional resources may be problematic – unknown and needs further testing</li><li>- Requires extra work on the admin and maintenance side</li></ul>
<b>Decision:</b>	<ul style="list-style-type: none"><li>• Moved to MVP due to complexity and to allow for more time to choose the best fit technologically</li></ul>	<ul style="list-style-type: none"><li>• Built first, as it is supported by current infrastructure</li><li>• Evaluate performance vs scalability</li></ul>

# **TYPOLOGIES AND RULES**

# The fraud risk typologies

## Typology 11: Money-laundering: Layering

 Attach  Create issue in epic  Link issue  Show draw.io Diagrams Panel

### Description

**Typology 11:** Money transfers from one account to numerous unrelated accounts. The immediate remittance or transfer of funds once they are deposited into an account.

Rule 017 Rule 086  
Rule 027 Rule 087

## Typology 27: SIM swaps

 Attach  Create issue in epic  Link issue  Show draw.io Diagrams Panel

### Description

**Typology 27:** Identity theft arising from fraudulent/offline SIM swaps that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling the fraudster to gain access to the consumer's mobile wallet and bank account.

Rule 003 Rule 016 Rule 030  
Rule 012 Rule 027 Rule 063

## Typology 28: Scams

 Attach  Create issue in epic  Link issue  Show draw.io Diagrams Panel

### Description

**Typology 28:** False promotions, phishing, or social engineering scams, such as fraudsters impersonating providers and advising customers that they have won a prize in a promotion and to send money to the fraudster's number to claim the prize.

Rule 009 Rule 014 Rule 030 Rule 048  
Rule 012 Rule 018 Rule 032 Rule 078

## Typology 214: Account muling





 Attach  Create issue in epic  Link issue  Show draw.io Diagrams Panel

### Description

**Typology 214:** The use of straw men (so-called "money mules"). A money mule is a natural person who makes his (bank) account available to a criminal or criminal organisation receiving some form of remuneration in return.

Rule 003 Rule 027 Rule 048  
Rule 012 Rule 030 Rule 078

## Rule: Implement Basic Blocklist Processing Engine

 Attach  Create subtask  Link issue  Show draw.io Diagrams Panel

### Description

Implement NodeJS/Deno+Redis as a Blocklist/Allowlist Provider

Block rule

# The APRICOT model, part IV

REFERENCE: 27

TYPE: FRAUD

MONEY LAUNDERING

**SUMMARY:**

Identity theft arising from fraudulent/offline SIM swaps that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling the fraudster to gain access to the consumer's mobile wallet and bank account.

**APRICOT CLASSIFICATION:**

<b>A</b>	Key Component	Concealing of identity	1	Victims	10 20 30 40 50 60 70 80 90 100
	Behavioural	Account changes		Participants	10 20 30 40 50 60 70 80 90 100
		Documentary discrepancies		Perpetrators	10 20 30 40 50 60 70 80 90 100
		Unauthorised access			10 20 30 40 50 60 70 80 90 100
	Suspect Transaction/s	Yes		Range	10 20 30 40 50 60 70 80 90 100
	Timeframe	Immediate		Visibility	10 20 30 40 50 60 70 80 90 100
<b>P</b>	Services	Digital financial services			

**DETAILED DESCRIPTION:**

A phone user's SIM is a reasonably stable and enduring component of their digital identity. From other economic activities, they will often install their previous SIM into the new phone to ensure continuity in their mobile access. As such, a SIM is also uniquely associated with a user's MSISDN (mobile number), which, in turn, is often used to uniquely identify the phone user for a variety of personal mobile services such as mobile money. A user's phone also provides a convenient external channel for two-factor authentication services.

If a user's SIM is lost or stolen, a criminal could potentially take over a user's mobile money account or intercept their SMS messages. The theft of a phone or SIM is not always possible, nor is it the easiest way to gain control of a user's SIM.

SIM swap occurs when a fraudster masquerades the customer service process to take over an user account with an MSISDN. The fraudster does this by requesting a SIM replacement or initiating a MSISDN porting order, enabling them to intercept SMS on a device that they own. The fraudster can then take advantage of using two-factor authentication to perform banking fraud, access mobile money accounts, and gain control of other third-party OTT accounts linked to the user through the SIM or MSISDN.

**SOURCES:**

<https://www.gsma.com/aboutus/workinggroups/what-is-sim-swap>  
<https://www.gsma.com/identity/wp-content/uploads/2020/10/GSMA-What-is-SIM-Swap.pdf>  
<https://www.theguardian.com/money/2020/sep/13/sim-swap-is-on-the-rise-how-can-you-stop-it-happening-to-you>

MITIGATION & MANAGEMENT STRATEGY:

PERSPECTIVE:

HUB

DFSP

AGENT

CUSTOMER

**Operational Controls**

- Customer education and communication to increase awareness of SIM swap risks
- Effective customer complaints monitoring, management and response
- Monitoring and flagging of account parties exhibiting suspicious behaviour
- Staff screening policies implemented by DFSPs
- Training of DFSP staff to combat customer social engineering
- DFSP system controls and protocols to prevent SIM swap without proper authentication and approval
- Implementation of effective customer identification/verification procedures to support of SIM swaps
- Implement a method of two-factor authentication for customers that is not device or MSISDN dependent
- Audit logging and reporting on SIM swap execution by the DFSP
- Check the distance between the active SIM location and the SIM swap execution location
- Strict controls on the recovery, availability of, and access to block SIM cards
- Control on far as reasonably feasible SIM swap execution
- Real-time monitoring, and alerting on SIM swap execution by the DFSP
- Monitoring and management of DFSP performance in implementing and managing operational controls
- Monitoring and management of high-risk associated processes (DFSP account alerts, balance enquiries, bank changes, etc.)
- Verification of the customer of high-risk processes associated against their MSISDN
- Automated transaction monitoring

**Transaction Monitoring**

- Evaluate all transactions coming into the wallet from a user and check for any irrational or anomalous behaviour

**Participant Monitoring**

- Review the paper information presented as part of a transaction and look for changes in relation to the paper's information from prior transactions that may indicate that a SIM swap had occurred

mojalo  
founda

# The data factory

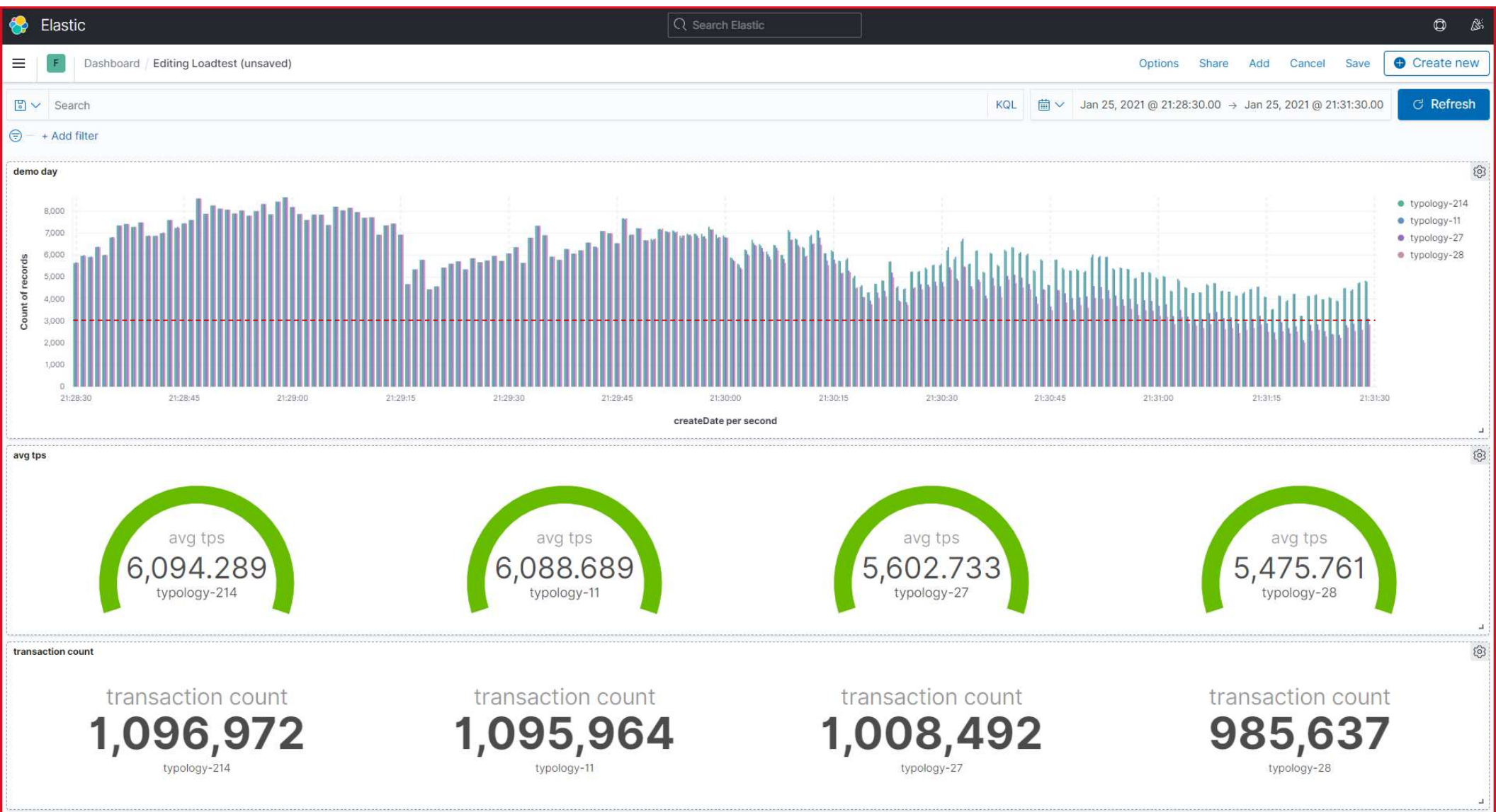
*We need to hide our Needle in a LOT of hay*

- Fraud and Typology Management see duplicate transactions as either:
  - A common pattern to be ignored
  - A suspicious pattern to be highlighted
- This creates a challenge - You run out of unique data very quickly at 10K TPS
  - 600K Transactions per minute
  - 36M Transactions per hour
  - 864M Transactions per day





# DEMO



# Improving performance

- Optimising the java-based components
- Re-evaluate the Kubernetes auto-scaler
- Define our telemetry/application performance management strategy
- To JSON or not to JSON
- Message compression

# Next steps

- Things we're addressing in the next sprint
  - A graph-capable rules engine
  - A performant historical data store
  - Rules configuration management and change control
  - Typology and rules orchestration
  - Improving performance
- Realistic data synthesis on a large scale
  - Simulate fraud without putting it there ourselves
  - Rule/Typology calibration
- Security and privacy
- Increased community participation
  - Secure onboarding and sharing of work and information