mojaloop

Fraud Risk Management

Program Increment 9 Report Out

21 April 2020

Contents

Introduction

Strategic assessment framework

Typologies classification

Typology Data requirements

Recommendations and next steps

Introduction

Fraud Risk Management (FRM) on the Mojaloop platform

PI 8

The Bill & Melinda Gates Foundation partnered with Deloitte to design a fraud risk management framework to work alongside Mojaloop to manage fraud and financial crime risks in a hyper-connected digital financial ecosystem

- Typology register and threat assessment using DREAD and STRIDE
- Data dictionary
- Business Requirements Document
- Illustrative KRI dashboard
- Proof of Concept

PI 9

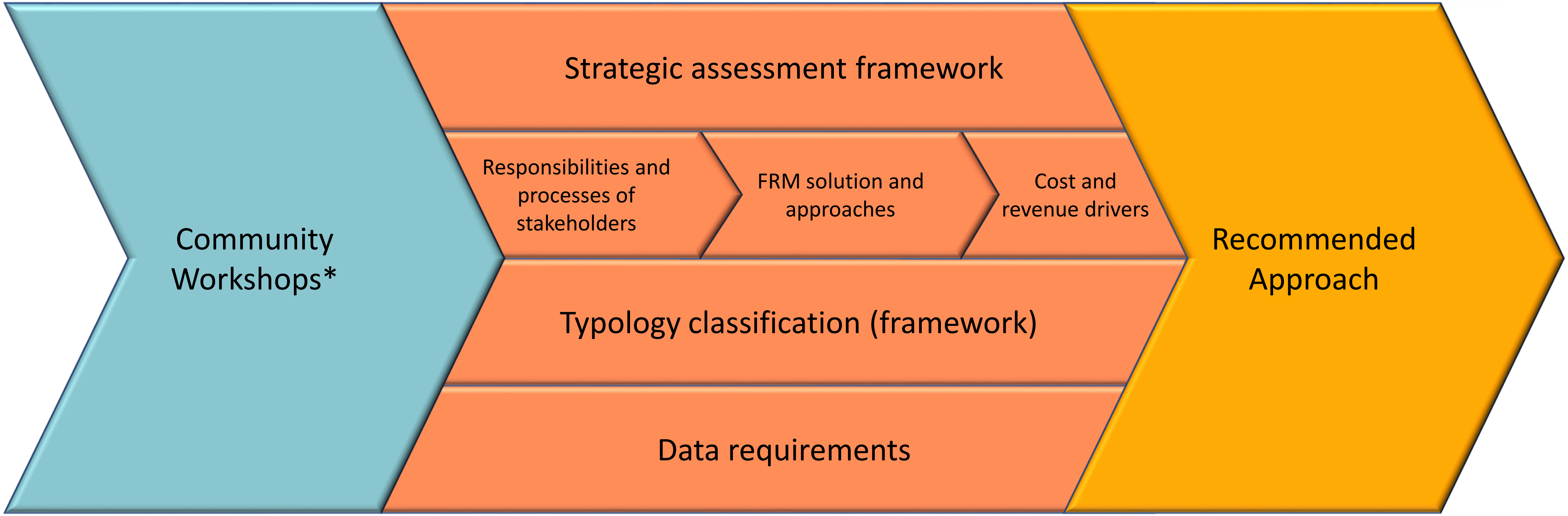
Fraud Risk was selected for further work "To review and classify the typologies to determine which of those strategically fit with Mojaloop's vision and how to get started building it"

- 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+

?

FRM solution strategy development approach



Community Workshops*

Strategic assessment framework

Responsibilities and processes of stakeholders

FRM solution and approaches

Cost and revenue drivers

Typology classification (framework)

Data requirements

Recommended Approach

* Special thanks to Aime, Rob and Dorota, Greg and Sudhir, as well as Simeon, Kim, Matt and Miller

Strategic assessment framework

Mojaloop strategy summary

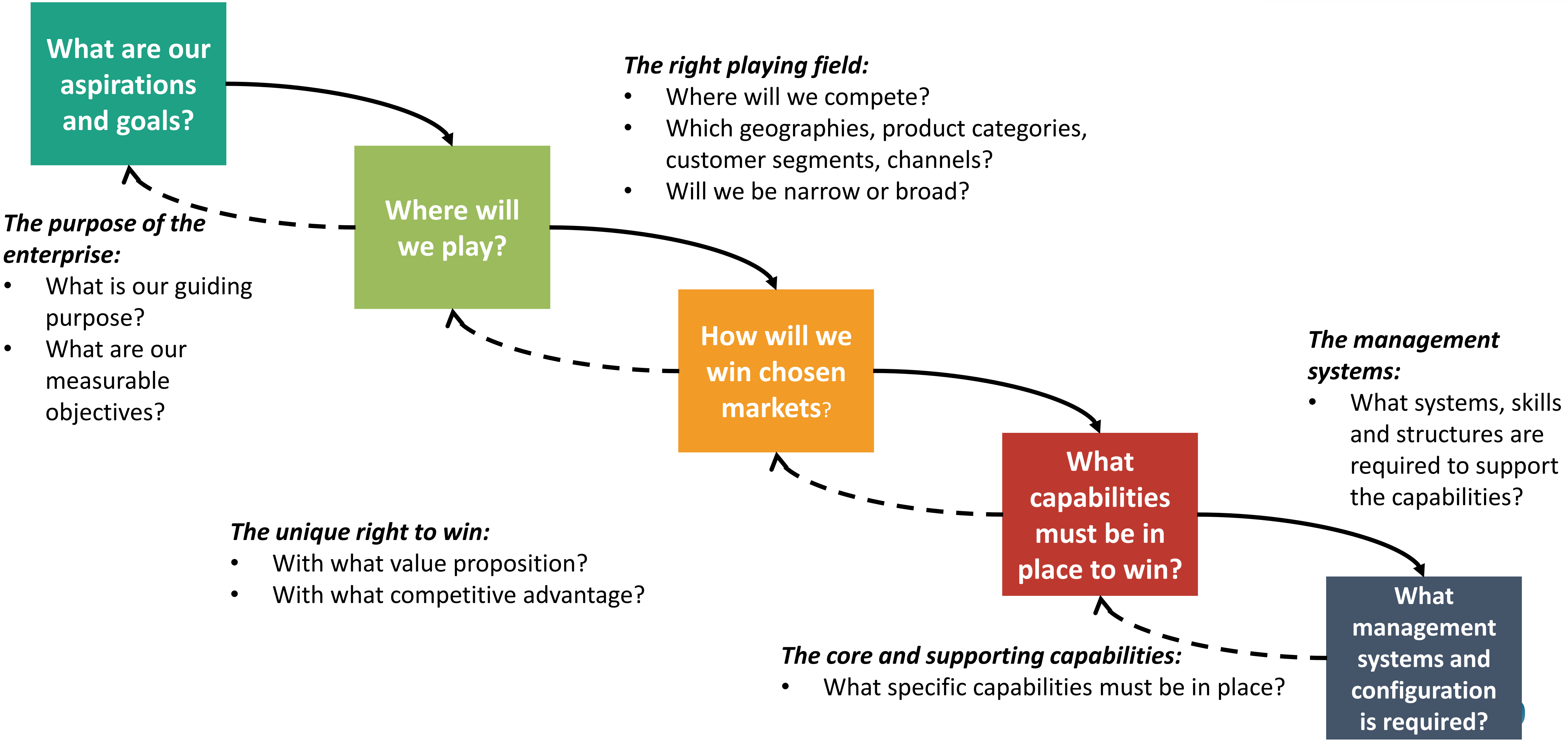
Stakeholders and FRM needs

FRM solution and approaches

Cost and revenue drivers

Cascading choices strategy methodology

Mojaloop strategy has been unpacked as a series of interrelated choices



What are our aspirations and goals?

The purpose of the enterprise:

- What is our guiding purpose?
- What are our measurable objectives?

Where will we play?

The right playing field:

- Where will we compete?
- Which geographies, product categories, customer segments, channels?
- Will we be narrow or broad?

How will we win chosen markets?

The unique right to win:

- With what value proposition?
- With what competitive advantage?

What capabilities must be in place to win?

The core and supporting capabilities:

- What specific capabilities must be in place?

What management systems and configuration is required?

The management systems:

- What systems, skills and structures are required to support the capabilities?

Mojaloop strategy summary

Goals and aspirations

Vision statement

A vision for a new, real-time digital payments system that supports inclusive digital and interoperable economies

Non-financial metrics

- Increased volumes
- Interoperability
- Cost efficiencies
- Faster transactions
- Financial inclusion

Financial metrics

“not-for-loss” or “cost-recovery-plus investment” basis

Where to play

Geography

- Global reach
- Africa and South East Asia
- Regional specific offices

Customer segments

“Bottom-of-the-pyramid” customers

How to win

Competitive advantage

- Access to digital financial services
- Low-cost payments systems
- Pan-continental interoperability
- Easy access via any device

Capabilities

Core capabilities

- Transparency - across the value chain to build trust
- Security
- Affordability Convenience
- Openness
- Robustness
- Integration
- Enable multiple use cases
- Knowledge transfer

Systems and configuration

- International payment standards
- Democratic governance structure
- Culture of accountability

Sources: Level one guiding principles, Mojaloop website

Stakeholders in the Mojaloop Ecosystem

Front end users

Digital financial service providers

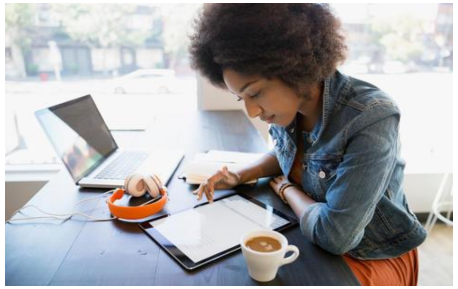
Mojaloop Hub Operators

Regulators

Stakeholders in the Mojaloop Ecosystem

Front end users: Users who send and receive payments via Mojaloop

Front End Users



Adebisi is a lawyer in Luanda Angola who sends part of her salary via her phone to her unemployed mother in rural Kalandula. She also buys groceries using her mobile wallet

FRM needs

- **Transaction safety**
- **Trusted agents**

Stakeholders in the Mojaloop Ecosystem

Digital financial service providers: The entity that serves as the connecting point between the front-end user and Mojaloop, in order to facilitate the transactions

DFSPs

Generic Bank is a FSP in Nigeria seeking to improve financial inclusion through the use of mobile wallets for the underserved. The bank reports to the payments authority and has a dedicated team that manages the ewallets

FRM needs

- **Fraud prevention, detection**
- **Fraud remediation**
- **Fraud reporting**

Stakeholders in the Mojaloop Ecosystem

Mojaloop Hub Operators: The entity enabling the functionality of the transaction through Mojaloop and maintaining the operations of the loop

Mojaloop Hub Operators

MIM

MIM is a mobile operator in East Africa who is entering the mobile payments market through the operation of the Mojaloop software. MIM is the connection point between the mobile wallets and bank accounts of the users

FRM needs

- **Fraud prevention**
- **Fraud detection**

Stakeholders in the Mojaloop Ecosystem

Regulators: The governing bodies and legislations that maintain the ethical and responsible functioning of the payment framework within which a Mojaloop implementation operates

Regulators

The African Reserve Bank is the central bank of Africa. The ARB is responsible for the formulation and implementation of monetary policy and can use its mandate to promote digital payments transactions

FRM needs

- **Standardisation of processes**
- **Adherence to fraud policies**

FRM Types

FRM benefits all stakeholders in varying degrees, with each having a unique role to play in FRM implementation

Does not need to implement with high benefits

Front end user	
Uses Mojaloop for payments?	Yes
Requires FRM?	Yes
Implements FRM?	No
Benefits from FRM?	High

Needs to implement with high benefits

DFSP	
Uses Mojaloop for payments?	No
Requires FRM?	Yes
Implements FRM?	Yes
Benefits from FRM?	High

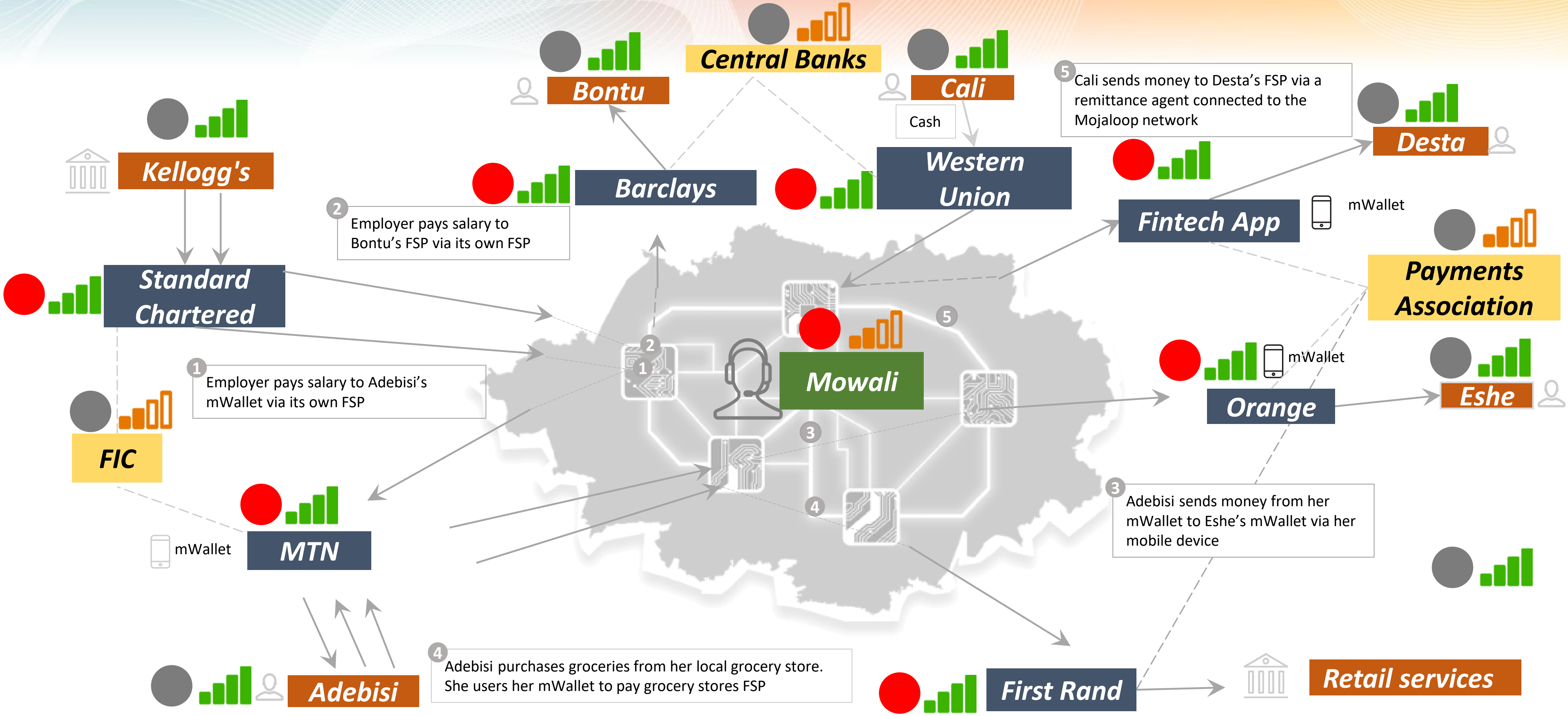
Needs to implement with moderate benefit

Operators	
Uses Mojaloop for payments?	No
Requires FRM?	Yes
Implements FRM?	Yes
Benefits from FRM?	Moderate

Does not need to implement with moderate benefits

Regulators	
Uses Mojaloop for payments?	No
Requires FRM?	No
Implements FRM?	No
Benefits from FRM?	Moderate

Mojaloop Ecosystem – FRM needs overlay



1 Employer pays salary to Adebisi's mWallet via its own FSP

2 Employer pays salary to Bontu's FSP via its own FSP

3 Adebisi sends money from her mWallet to Eshe's mWallet via her mobile device

4 Adebisi purchases groceries from her local grocery store. She users her mWallet to pay grocery stores FSP

5 Cali sends money to Desta's FSP via a remittance agent connected to the Mojaloop network

Note: Organisation names used are indicative and for illustration purposes only

🟧 Front End Users 🟦 Digital Financial Service Provider 🟩 Mojaloop Hub Operators 🟨 Regulators

● Does not need to implement FRM 🔴 Needs to implement FRM ▂▄▆ Moderate Benefit ▂▄▆ High benefit

Stakeholder involvement in FRM

FRM activities are primarily performed by DFSP's, therefore the impact of the Mojaloop FRM solution on the DFSP should be considered at all times

Activities[1]		Stakeholders[3]			
		Front end	DFSP	Operator	Regulator
Diagnose Proactive measures implement to deter or obstruct the committing of fraud	Diagnose vulnerability to fraud	◕	●	●	◔
	Develop a strong risk management environment	○	●	●	◕
	Create fraud prevention policies and activities	○	●	◕	●
	Create a culture of honesty and integrity	◕	●	◕	◕
Detect A set of activities undertaken to prevent money or property from being obtained through false pretences	Continuous or periodic monitoring	◔	●	●	◔
	Detect gaps in anti-fraud controls	◔	●	◕	◔
	Establish fraud risk profiles	◔	●	◕	◔
	Fraud hotline mechanisms	●	●	◕	◔
Respond Policies, procedures and activities that allow the organization to react to various types of fraud and misconduct allegations in a measured and consistent manner	Recommend Mitigating Anti-fraud Controls	◔	●	●	◕
	Develop Fraud Response Plan	◔	●	●	◔
	Investigate cases of alleged fraud	◔	●	◕	◕
	Fraud reporting statutory	◔	●	●	●
	Incorporate identified fraud risks into FRM framework	◕	●	◕	●
	Overall involvement in FRM	◔	●	●	◕

Insights

Although all players in the ecosystem have some responsibility towards fraud management it would appear that the **bulk of the burden** lies with the **DFSPs**

Consideration should be given to the **impact** on the **DFSPs** for **any FRM solution** implemented by the Operator as well as the interfaces between the two

Key[2]
(Involvement in Mojaloop FRM)

○	Low degree of involvement
◔	Some degree of involvement
◕	Moderate degree of involvement
●	High degree of involvement

Notes:

[1] Based on the Deloitte FRM framework in conjunction with CIMA guidelines

[2] All assessments are made from the point of view of the loop operator considering the involvement of stakeholders across the ecosystem

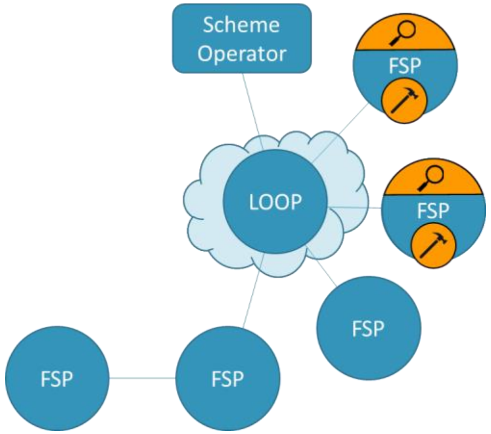
[3]Assessments have been allocated with consideration given to varying stakeholder types as well as results of the typologies work

As the process matures, consideration will be given to other FRM participants such as specialised security response centres

mojaloop

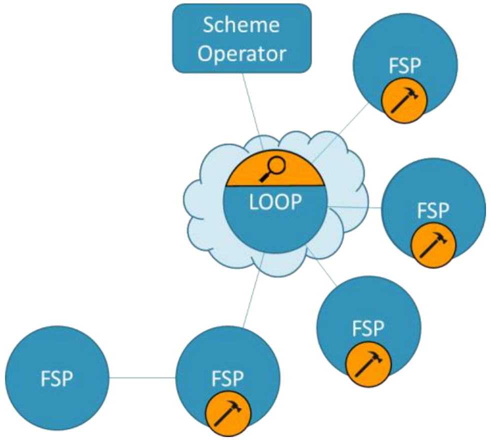
Operating model configurations

Depending on a Mojaloop operator’s operating environment and participants, Fraud Risk Management services can be provisioned through an appropriate operating model



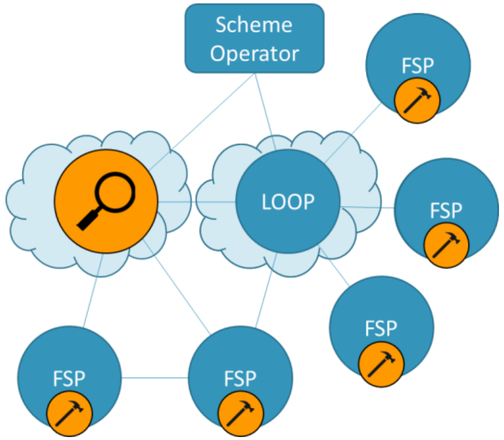
Distributed (AS IS)

- 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



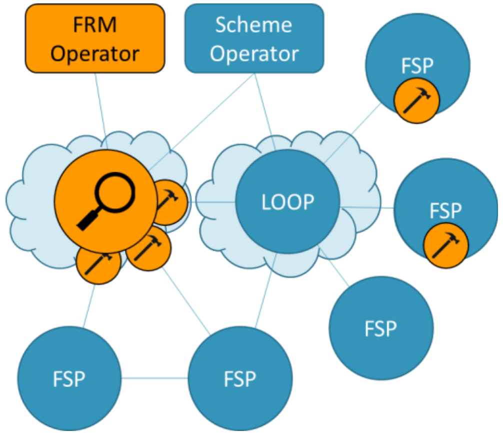
Embedded (BRD)

- 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

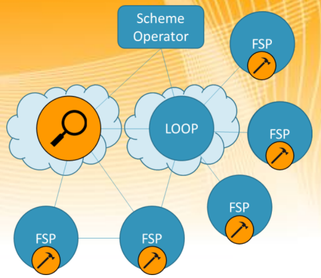
- Centralised fraud risk detection service hosted by the switch Operator
- Separate interface to receive transactions from switch participants and non-participants
- The Operator performs detection on all transactions routed to the FRM service
- Each FSPs would employ compliance teams



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

Semi-Attached FRM operating model approach



Operating model type: Semi-Attached

Model description:
Centralised open-access fraud detection (Mojaloop Hub Operator); Distributed compliance functions (DFSPs)

Where to play

Design Features

- The Operator automatically evaluates every "switched" transaction
- The Operator also evaluates every "non-switched" transaction submitted specifically for fraud detection
- The Operator blocks accounts for suspicious "switched" transactions after the transaction is concluded
- The Operator notifies the DFSP(s) of the suspicious transaction with an alert
- The DFSP(s) investigate and resolve alerts

Use cases

- Allow smaller DFSPs access to a more regulated and ubiquitous platform without the high cost of entry associated with traditional toolsets
- Where systemic fraud exploiting the blind-spots between DFSPs is prevalent
- Where unregulated, smaller and informal DFSPs is prevalent
- Where peer-to-peer transactions between DFSPs are prevalent or popular

How to win

Value proposition

Operator
- Added value
- Trust assurance
- Inclusion through lower costs
- Wider reach
- Increased revenue opportunities

DFSP's
- Compliance
- Cost savings
- Access to FRM services

Front end Users
- Money safety
- Low costs

Regulators
- Wider view
- Standardisation
- Modernisation

Key dependencies

- Effective KYC/EDD
- Enforceable contracts and service level agreements
- Transparent processes
- Data availability

Capabilities

Core capabilities

Technical
- Rules Engine
- Process automation
- Data management
- UI Access
- Open FRM interface

Non-technical
- Contracts management
- Stakeholder management

Systems and skills

- **People and Processes:**
- Administrators and supervisors
- Rules configurer
- Change control
- **Systems (i.e. technical):**
- Rules Engine
- Workflow
- Case Management

Risks and constraints

Risks
- Poor KYC/EDD
- Unregulated FSPs
- Privacy compliance

Constraints
- Lack of formal regulation
- Implementation and operational costs

Management systems and configurations

Stakeholder involvement

FSP -
- Submit ALL transactions
- Submit participant information
- Manage alerts

Front end user –
- None directly – users would interact through their FSPs
- Information provision

Regulator –
- None directly – FSPs would engage the regulator

Implementation cost

- Time & Materials deployment
- Cloud infrastructure
- Bandwidth/connectivity

Time to implement

- 6 to 18 months

Financial model – cost drivers

The semi attached and embedded approach are considered cost optimal when considered along with the benefit received from each solution

		FRM Approach			
		Distributed	Embedded	Semi-attached	Standalone
Investment costs	Software development	○	◔	◔	●
Implementation costs	Legal fees	○	◔	◕	●
	Licensing - initial procurement cost	○	○	○	◔
	Infrastructure costs	○	◔	◔	●
	Customisation	○	◔	◔	●
Running costs	Training	◔	◕	◕	●
	Staffing	○	◔	◔	●
	Maintenance support	○	○	○	◕
	Software updates	○	○	○	◕
	Licensing - renewal cost	○	○	○	◔
	Compliance	○	○	○	◕
Overall cost requirements		○	◔	◔	●

Key

○	No significant cost requirement
◔	Low cost requirement
◕	Moderate cost requirement
●	High cost requirement

Financial model – revenue drivers

		FRM Approach			
		Distributed	Embedded	Semi-attached	Standalone
Revenue types	FRM Transaction fee	○	◔	◔	●
	FRM Fixed fee	○	◔	◕	●
	Supporting data fee	◔	◕	◕	◔
Overall potential for revenue generation		◔	◔	◕	●

Key

○ No revenue potential ◔ Low revenue potential ◕ Moderate revenue potential ● High revenue potential

Key takeaways

Why Fraud Risk Management on the Mojaloop platform?

- Centralised services for lower (shared) implementation and operating costs
- Build trust in digital financial services by assuring the safety and security of digital financial transactions through transparency across the value chain
- Standardisation and modernisation of fraud detection solutions

Typology classification

Typology classification framework

Execution, outcomes and insights

Examples

Typology classification

Fraud Risk Management on the Mojaloop platform

PI 8

The Bill & Melinda Gates Foundation partnered with Deloitte to design a fraud risk management framework to work alongside Mojaloop to manage fraud and financial crime risks in a hyper-connected digital financial ecosystem

- Typology register and threat assessment using DREAD and STRIDE
- Data dictionary
- Business Requirements Document
- Illustrative KRI dashboard
- Proof of Concept demo

PI 9

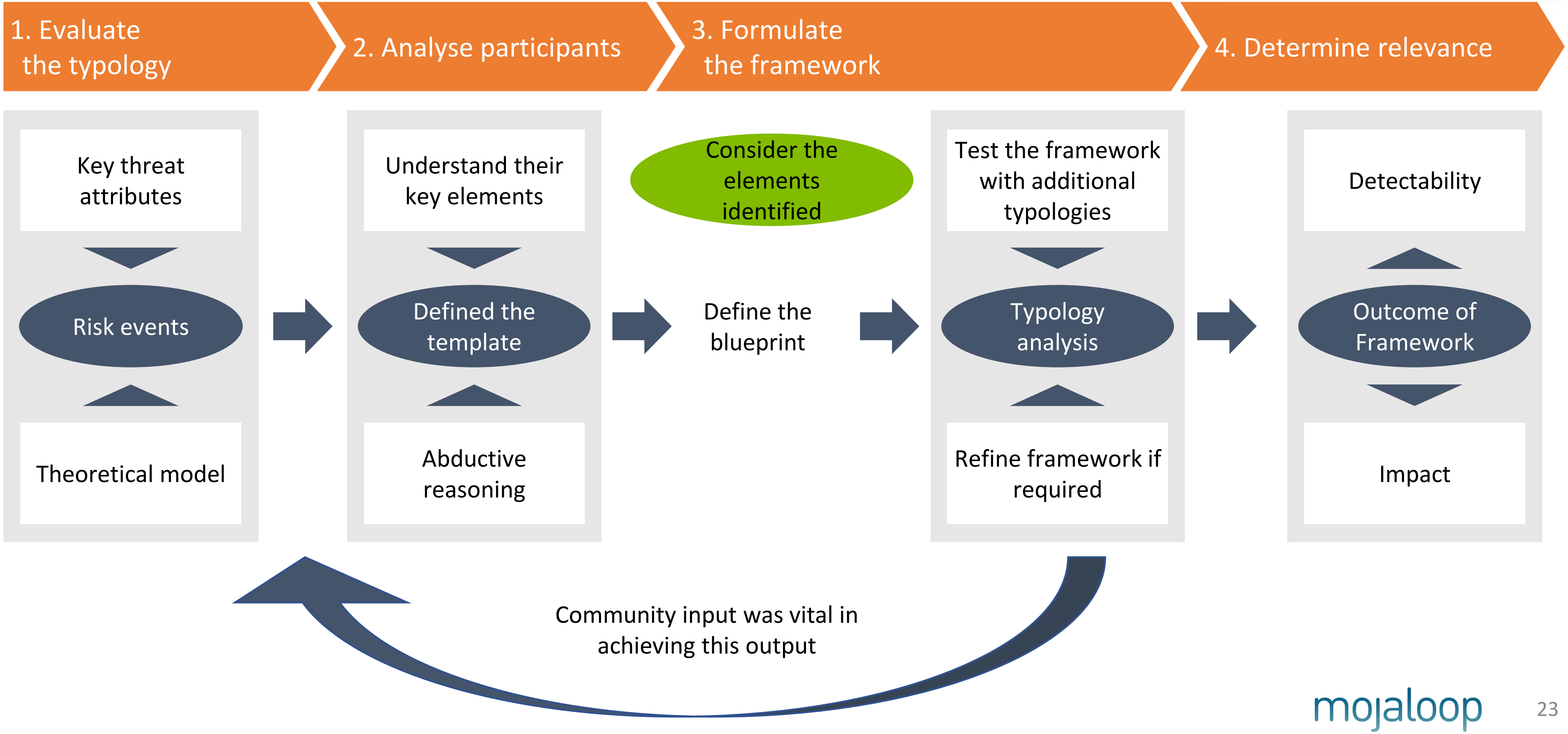
Fraud Risk was selected for further work "To review and classify the typologies to determine which of those strategically fit with Mojaloop's vision and how to get started building it"

- The development of a strategic assessment framework
- **The detailed classification of the risk typologies already identified to determine those that are relevant to a typical Mojaloop implementation**
- A detailed cross-reference between the risk typologies and the data dictionary already developed

PI 10+

?

Threat modelling approach



1. Evaluate the typology

2. Analyse participants

3. Formulate the framework

4. Determine relevance

Key threat attributes

Risk events

Theoretical model

Understand their key elements

Defined the template

Abductive reasoning

Consider the elements identified

Define the blueprint

Test the framework with additional typologies

Typology analysis

Refine framework if required

Detectability

Outcome of Framework

Impact

Community input was vital in achieving this output

Theoretical applicability framework

A

Approach

- Defines the process attributes that are utilised as part of the typology
- Examples
  - Multiple Transactions
  - Foreign Parties

P

Product / Service

- Defines whether the typology is limited to a specific product
- Examples
  - Check Account
  - Savings Account

R

Regulatory Impact

- Defines whether the typology is a result of / circumvention of regulatory threshold
- Examples
  - Limits

I

Involved Parties

- Defines the actors / participants that are involved in the typology
- Examples
  - User
  - Agent

C

Channel

- Defines the criteria in which the typology interacts with the DFSP
- Examples
  - Internet
  - Face-to-face
  - Non face-to-face

O

Organisational Scope

- Defines the criteria that provides context to the other elements
- Examples:
  - Behavioural aspects

T

Transaction Type

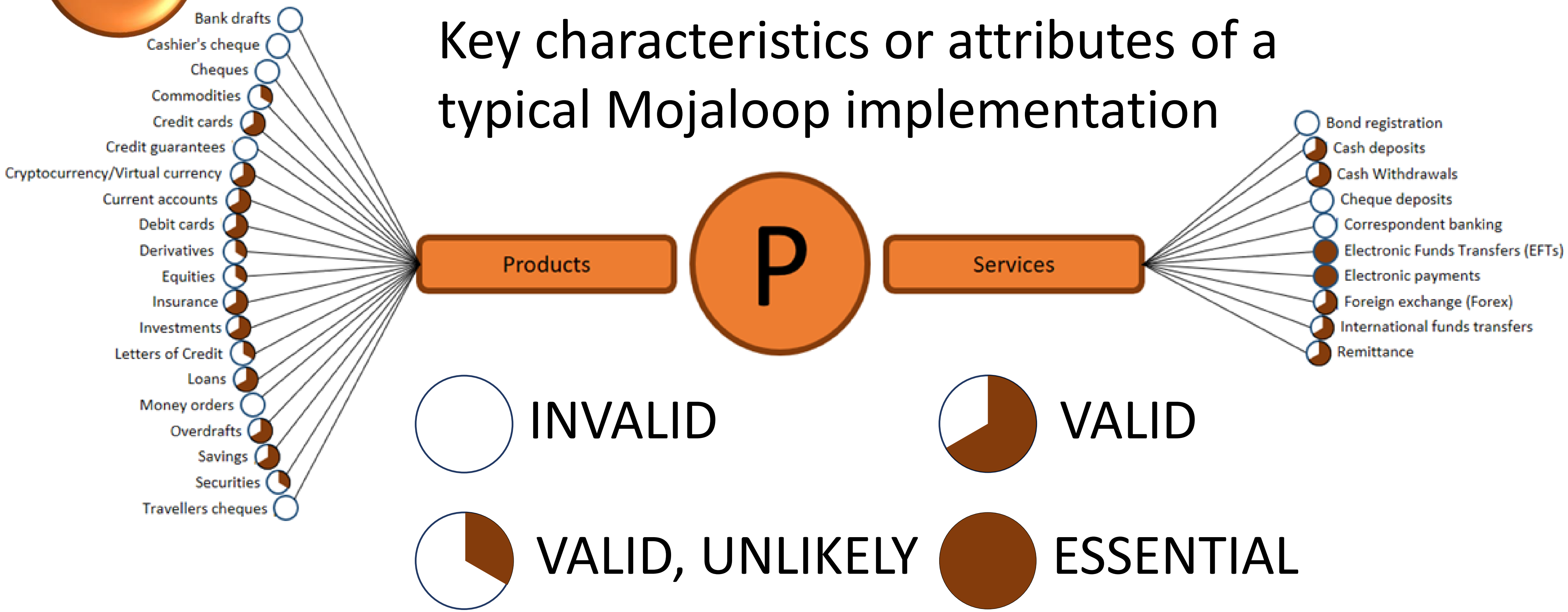
- Defines the type of transactions that are utilised to perform the typology
- Examples
  - Transfer
  - Payment
  - Deposit

mojaloop

A break down of each element

P PRODUCTS/SERVICES

Key characteristics or attributes of a typical Mojaloop implementation



P

Products

- Bank drafts ○
- Cashier's cheque ○
- Cheques ○
- Commodities ◔
- Credit cards ◕
- Credit guarantees ○
- Cryptocurrency/Virtual currency ◕
- Current accounts ◕
- Debit cards ◕
- Derivatives ◔
- Equities ◔
- Insurance ◕
- Investments ◕
- Letters of Credit ◔
- Loans ◕
- Money orders ○
- Overdrafts ◕
- Savings ◕
- Securities ◔
- Travellers cheques ○

Services

- ○ Bond registration
- ◕ Cash deposits
- ◕ Cash Withdrawals
- ○ Cheque deposits
- ○ Correspondent banking
- ● Electronic Funds Transfers (EFTs)
- ● Electronic payments
- ◕ Foreign exchange (Forex)
- ◕ International funds transfers
- ◕ Remittance

○ INVALID

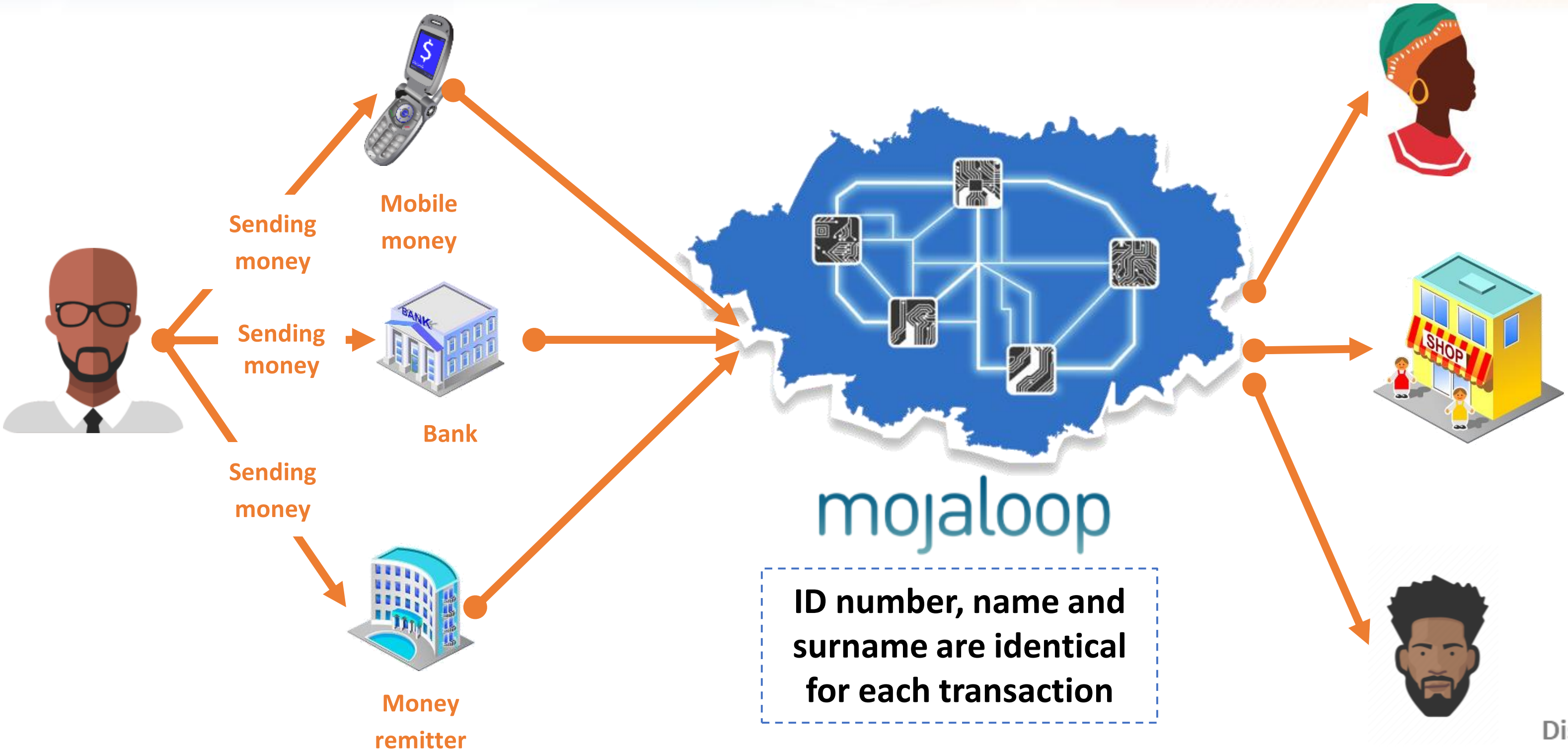
◕ VALID

◔ VALID, UNLIKELY

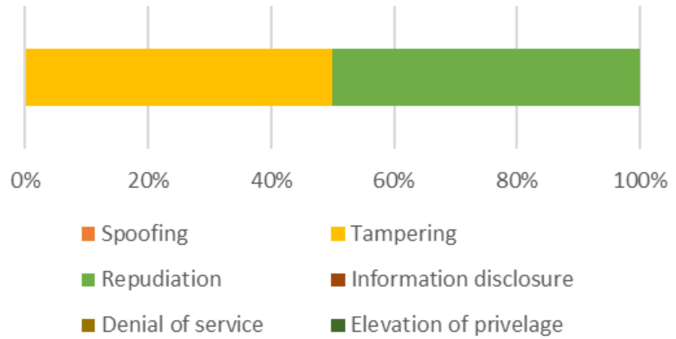
● ESSENTIAL

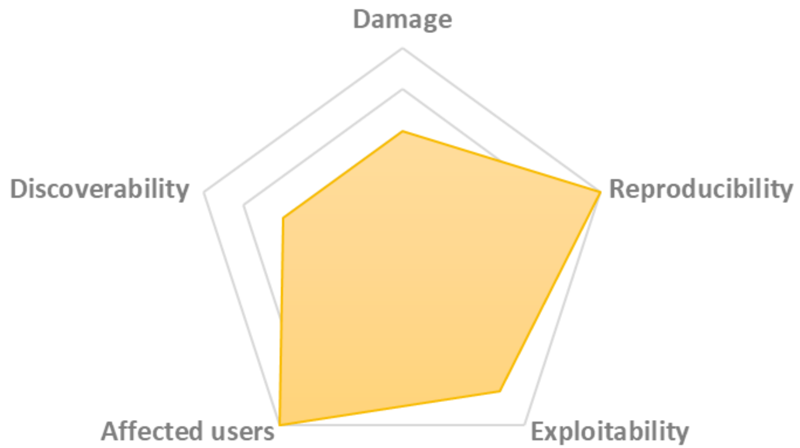
mojaloop

Review of Selected Typologies #1



ID number, name and surname are identical for each transaction

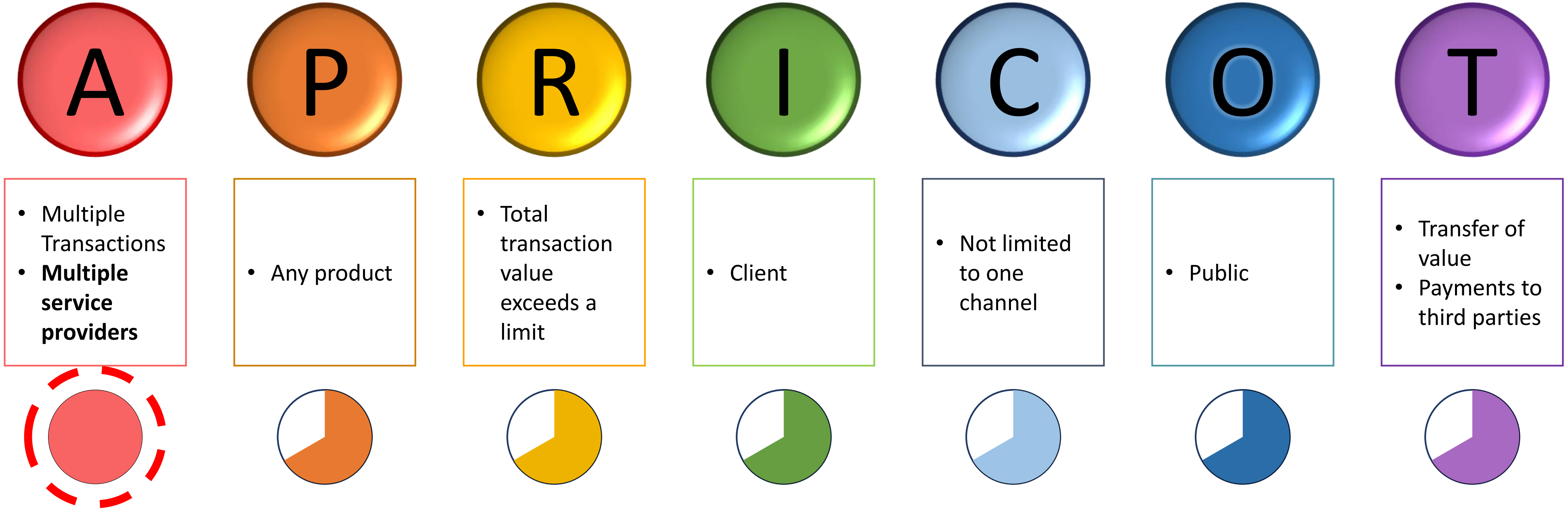




Sending multiple transactions through different Money or Value transfer (MVT) service providers to conceal the value of total funds being remitted to circumvent set thresholds

Review of Selected Typologies #1

Sending **multiple transactions** through **different Money or Value transfer (MVT) service providers** to conceal the value of total funds being remitted to **circumvent set thresholds**



A

- Multiple Transactions
- **Multiple service providers**

P

- Any product

R

- Total transaction value exceeds a limit

I

- Client

C

- Not limited to one channel

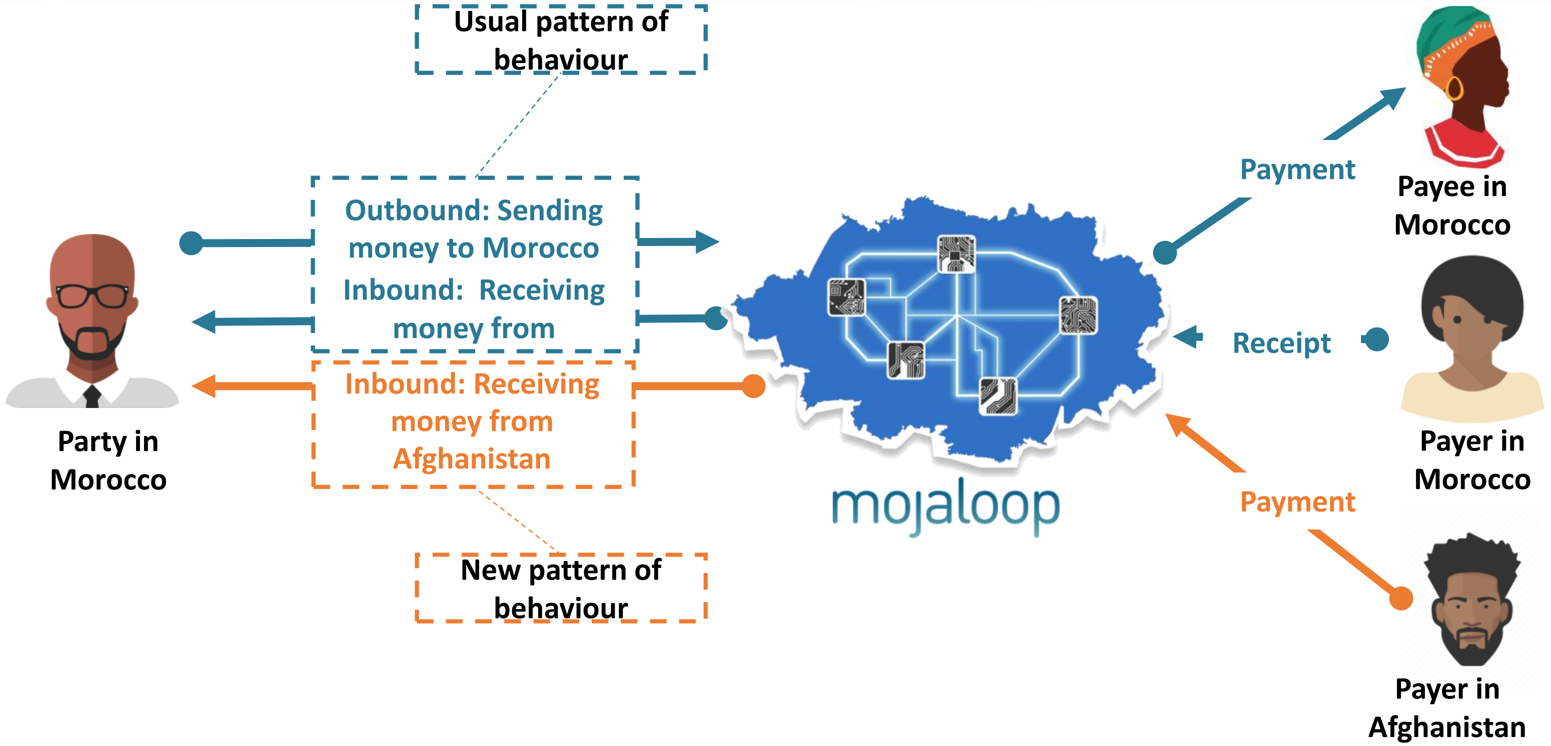
O

- Public

T

- Transfer of value
- Payments to third parties

Review of Selected Typologies #2



Usual pattern of behaviour

Outbound: Sending money to Morocco

Inbound: Receiving money from

Inbound: Receiving money from Afghanistan

New pattern of behaviour

Party in Morocco

mojaloop

Payment

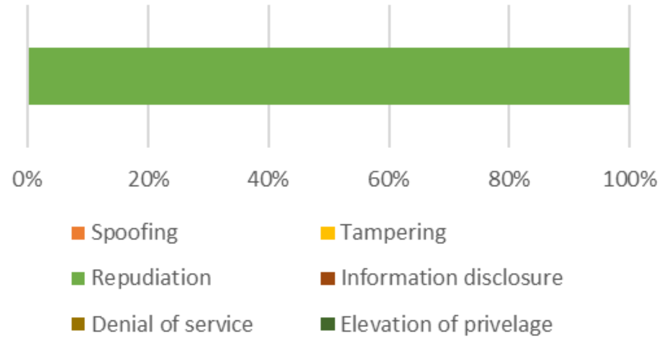
Payee in Morocco

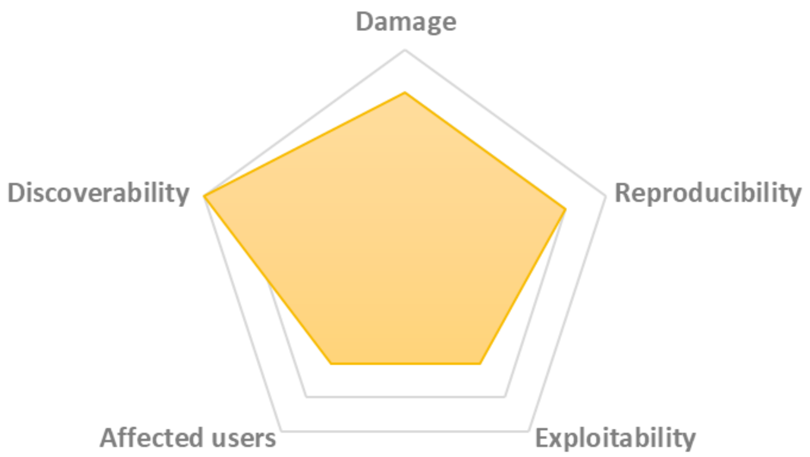
Receipt

Payer in Morocco

Payment

Payer in Afghanistan



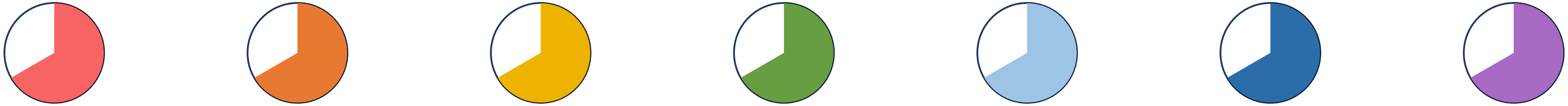


Unwarranted desire to involve entities in foreign jurisdictions in transactions. International transfers received from/sent to foreign countries not in accordance with the profile of the customer.

Review of Selected Typologies #2 – Standard view

Unwarranted desire to involve entities in foreign jurisdictions in transactions. **International transfers** received from/sent to **foreign countries not in accordance with the profile** of the customer.

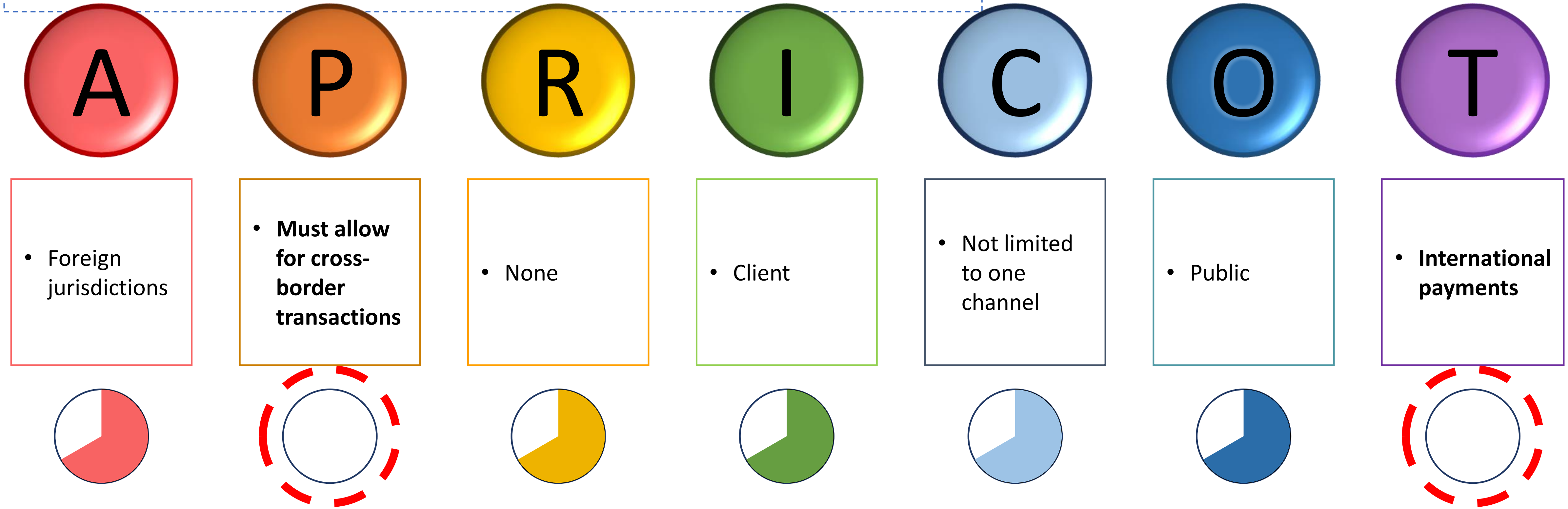
A	P	R	I	C	O	T
• Foreign jurisdictions	• Must allow for cross-border transactions	• None	• Client	• Not limited to one channel	• Public	• International payments



Assumption: The implementation allows for cross border payments

Review of Selected Typologies #2 – An alternative

Unwarranted desire to involve entities in foreign jurisdictions in transactions. **International transfers** received from/sent to **foreign countries not in accordance with the profile** of the customer.



- Foreign jurisdictions

- **Must allow for cross-border transactions**

- None

- Client

- Not limited to one channel

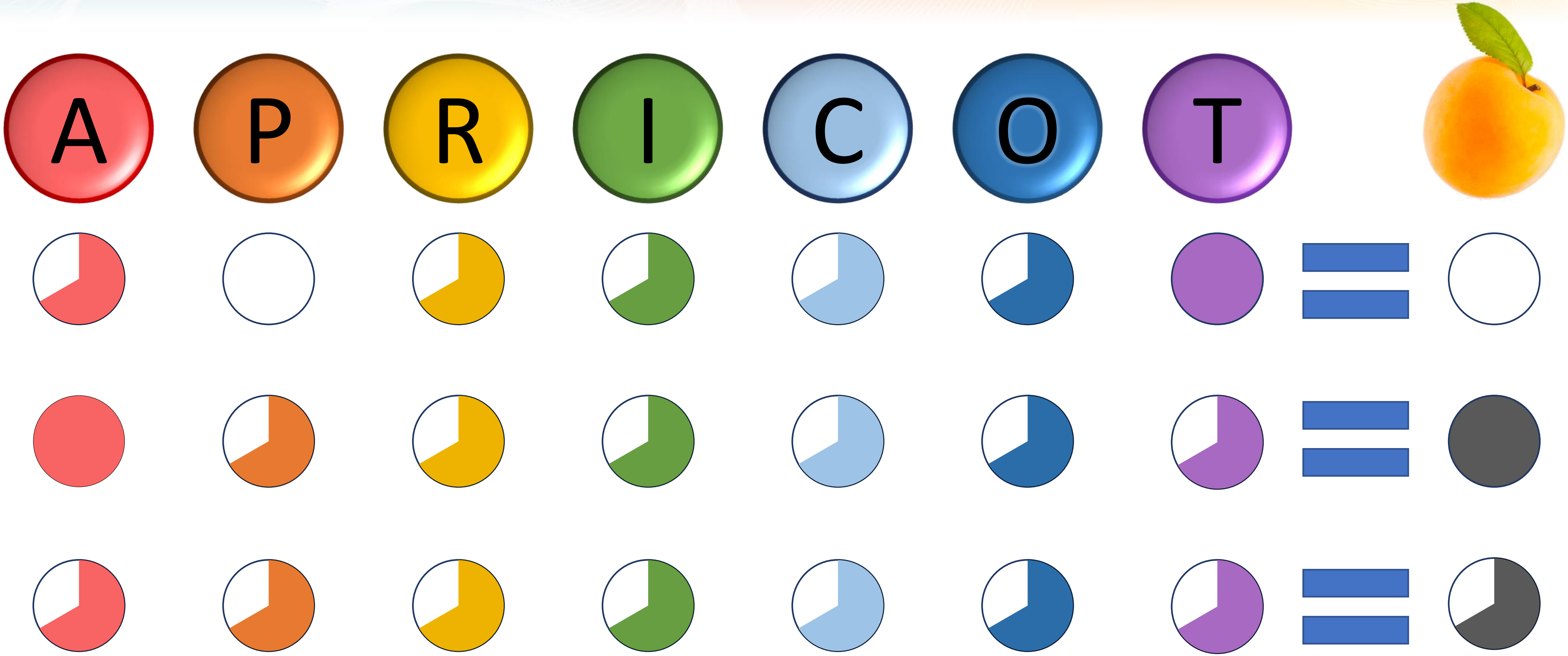
- Public

- **International payments**

Assumption: The implementation does **not** allow for cross border payments

The outcome of the review is therefore based on the template utilised for the Operator

Flexibility of framework



Key takeaways

- A flexible framework that can be utilised to assess typologies for any implementation
- Development of a foundation to generate appropriate insights on which a Fraud Risk Management Solution can be built
- The information gathered through fraud risk management will enable a different lens on the payment processing data

Typology data requirements

DAMA standardisation

Data requirements

Typology data requirements breakdown

Payer

- Direct identification information
  - Name
  - Foundational ID
- Secondary identification information
  - SIM/Device
  - IP address
  - Email address
  - Phone number
  - Account number
- Location information
  - Country
  - IP address
  - Physical address
- Descriptive data
  - Occupation
  - PEP status
  - Source of Wealth

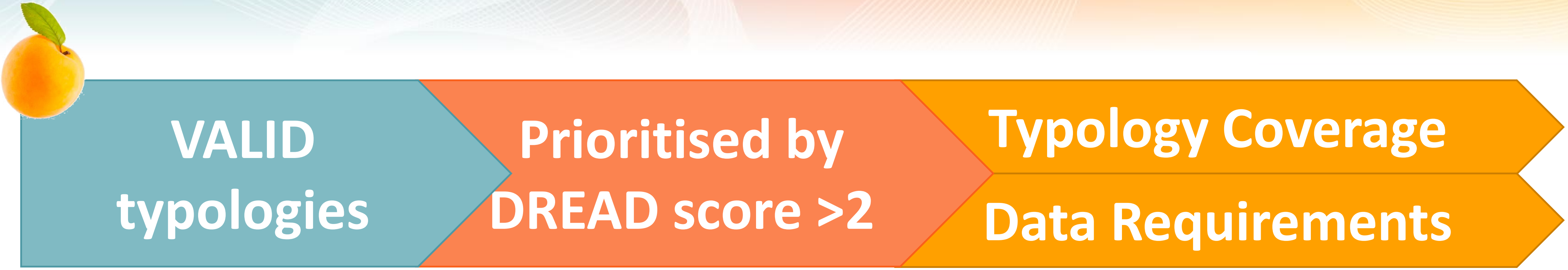
Transaction

- Identification information
  - Payer
  - Payee
  - Agent
- Location information
  - Source
  - Destination
- Descriptive data
  - Reference
  - Currency
  - Amount

Payee

- Direct identification information
  - Name
  - Foundational ID
- Secondary identification information
  - SIM/Device
  - Phone number
  - Account number
- Location information
  - Country
  - Physical address
- Descriptive data
  - PEP status
  - Source of Wealth

Typology data requirements breakdown



VALID typologies

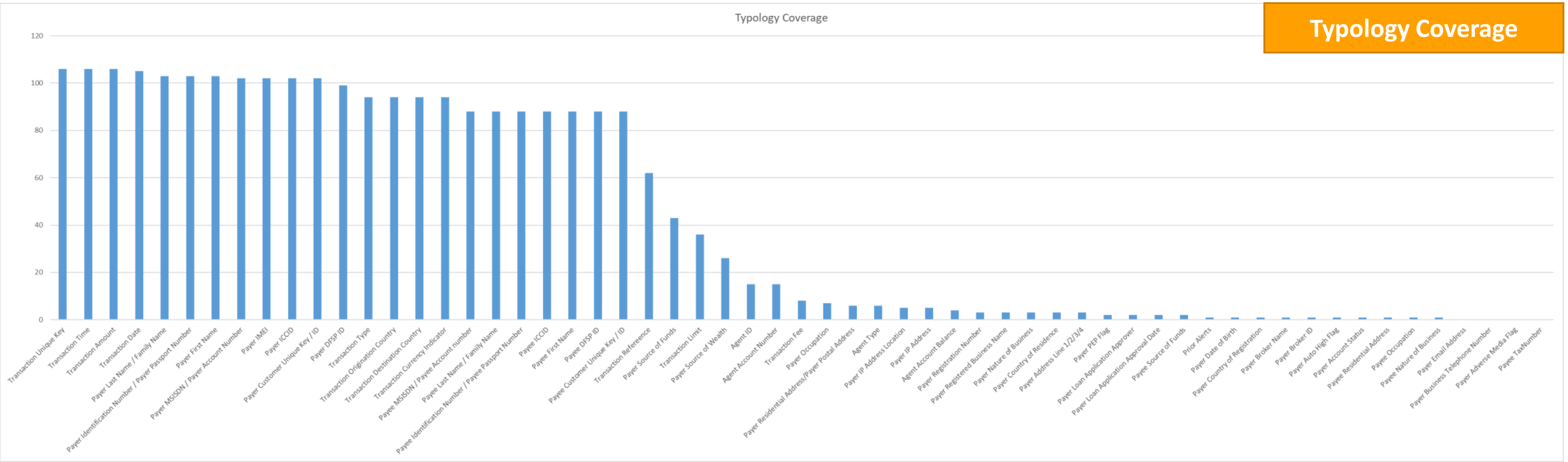
Prioritised by DREAD score >2

Typology Coverage

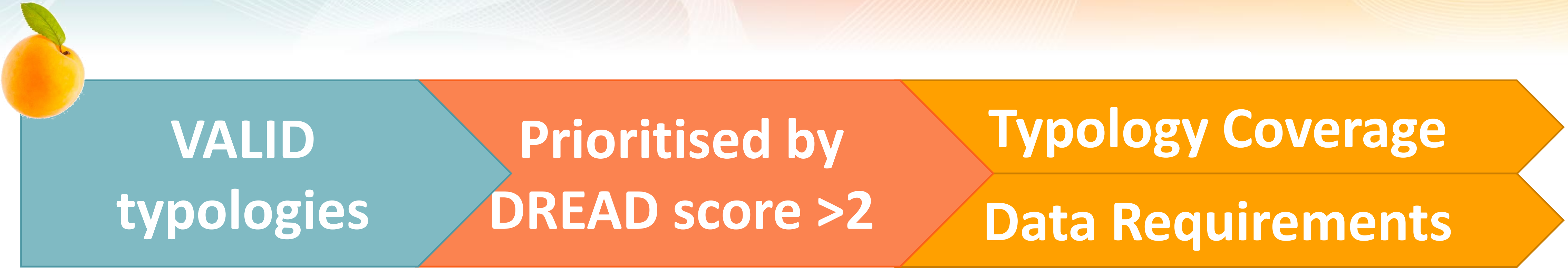
Data Requirements

126/232

109/126



Typology data requirements breakdown



VALID typologies

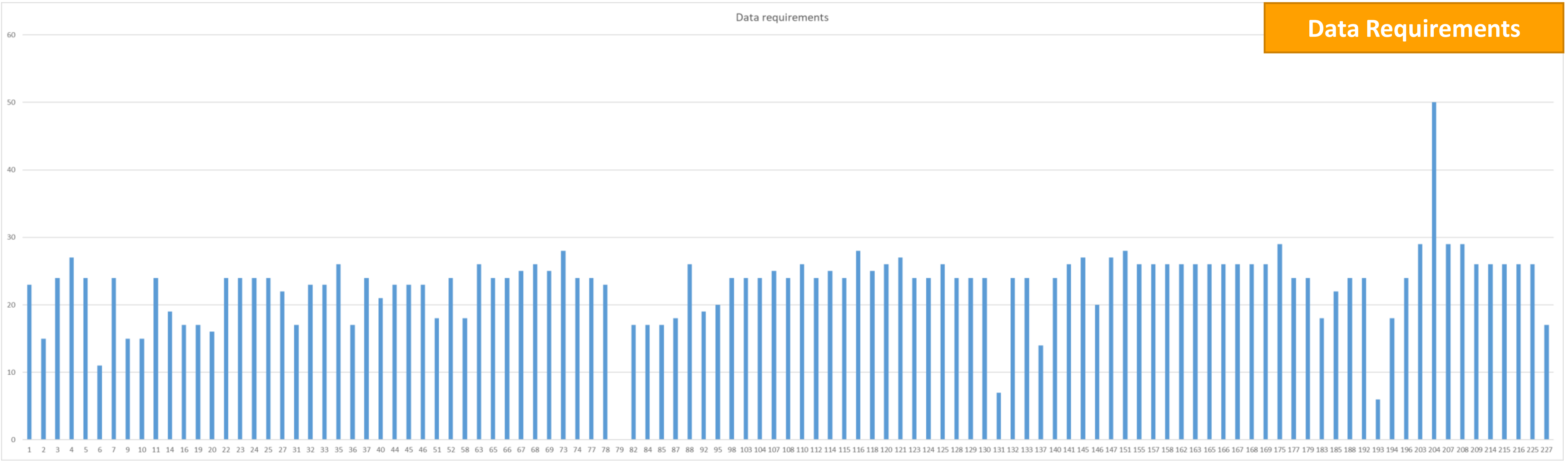
Prioritised by DREAD score >2

Typology Coverage

Data Requirements

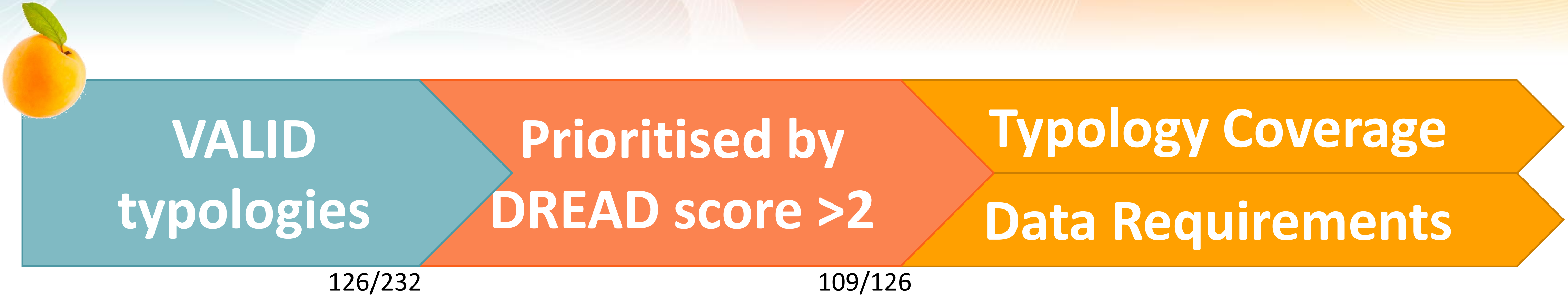
126/232

109/126



Data Requirements

Typology data requirements breakdown



VALID typologies

Prioritised by DREAD score >2

Typology Coverage

Data Requirements

126/232

109/126

- With half of the fields, we can detect 74 typologies
- However, we lose
  - 17 typologies with DREAD scores less than 3
  - 12 typologies with DREAD scores between 3 and 4
  - 6 typologies with DREAD scores greater than 4

Recommendations and next steps

FRM – Where to from here?

1

- Select the Semi-Attached approach for a Fraud Risk Management solution to complement Mojaloop switching services
- Solve for the dependency on quality KYC/EDD information

2

- Prioritise VALID typologies for development
- Document the typology rules in readable pseudo-code
- Design system and operational controls for VALID typologies

3

- Grade the effectiveness of typology detection based on real data availability

Recommendations and next steps

FRM – Where to from here?

4

- Prioritise the development of a rules engine service component
- Review the need for a general Mojaloop Case Management service component

5

- DFSPs and prospective operators should evaluate their role and responsibilities for effective fraud risk management within the Mojaloop platform