mojaloop

Fraud Risk Management Framework

Mojaloop OSS Community Convening

January 2020

Project scope, context and deliverables

- Mojaloop was developed to enable customers to send digital payments to anyone, regardless of the account or service they use by making it easier for financial providers to achieve interoperability

- 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

DFSP

Payer

mojaloop

Payee

Customer Data

Transactional/ Product Data

Recipient Data

Data Collection

Typology Data Dictionary

Ongoing Monitoring

Key Risk Indicator Dashboard

Transaction Monitoring

Fraud/AML Typologies

SAS POC

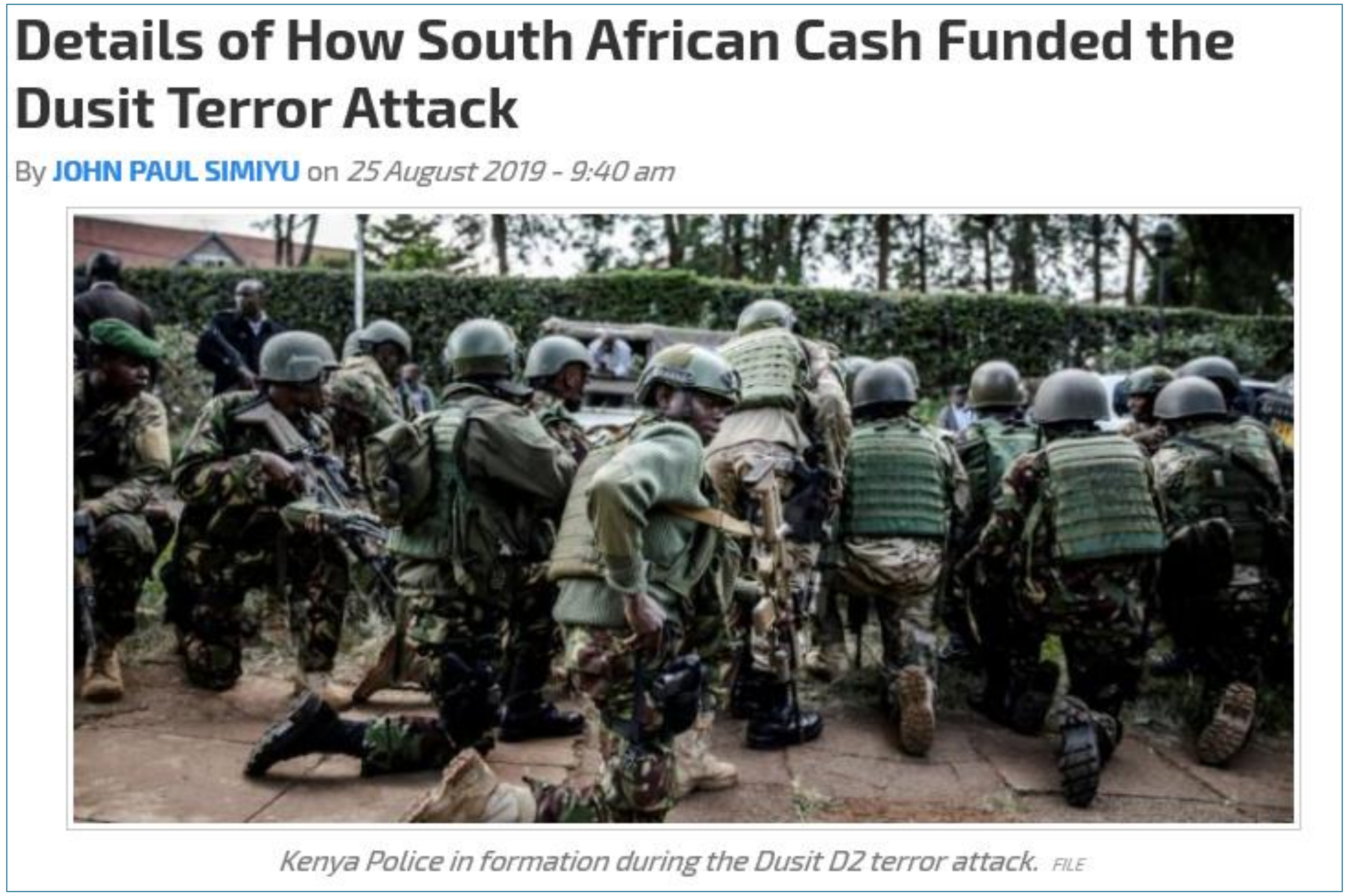
Risk Rating of Typologies

Risk Alerts & Suspicious Transaction Information

Business Requirements Document

Risk ranking methodology and typologies

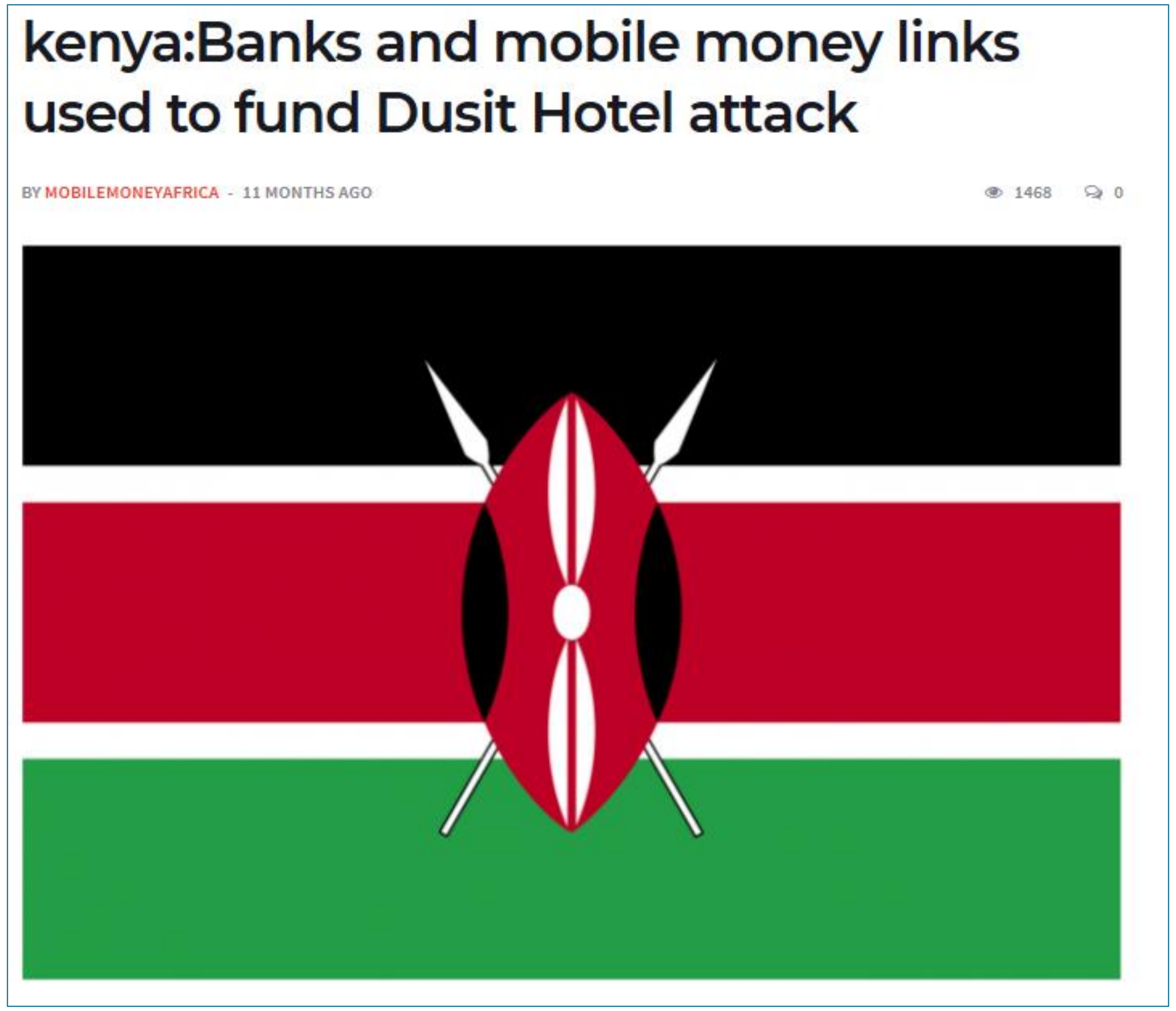
Risks in the mobile payments ecosystem



Details of How South African Cash Funded the Dusit Terror Attack

By JOHN PAUL SIMIYU on *25 August 2019 - 9:40 am*

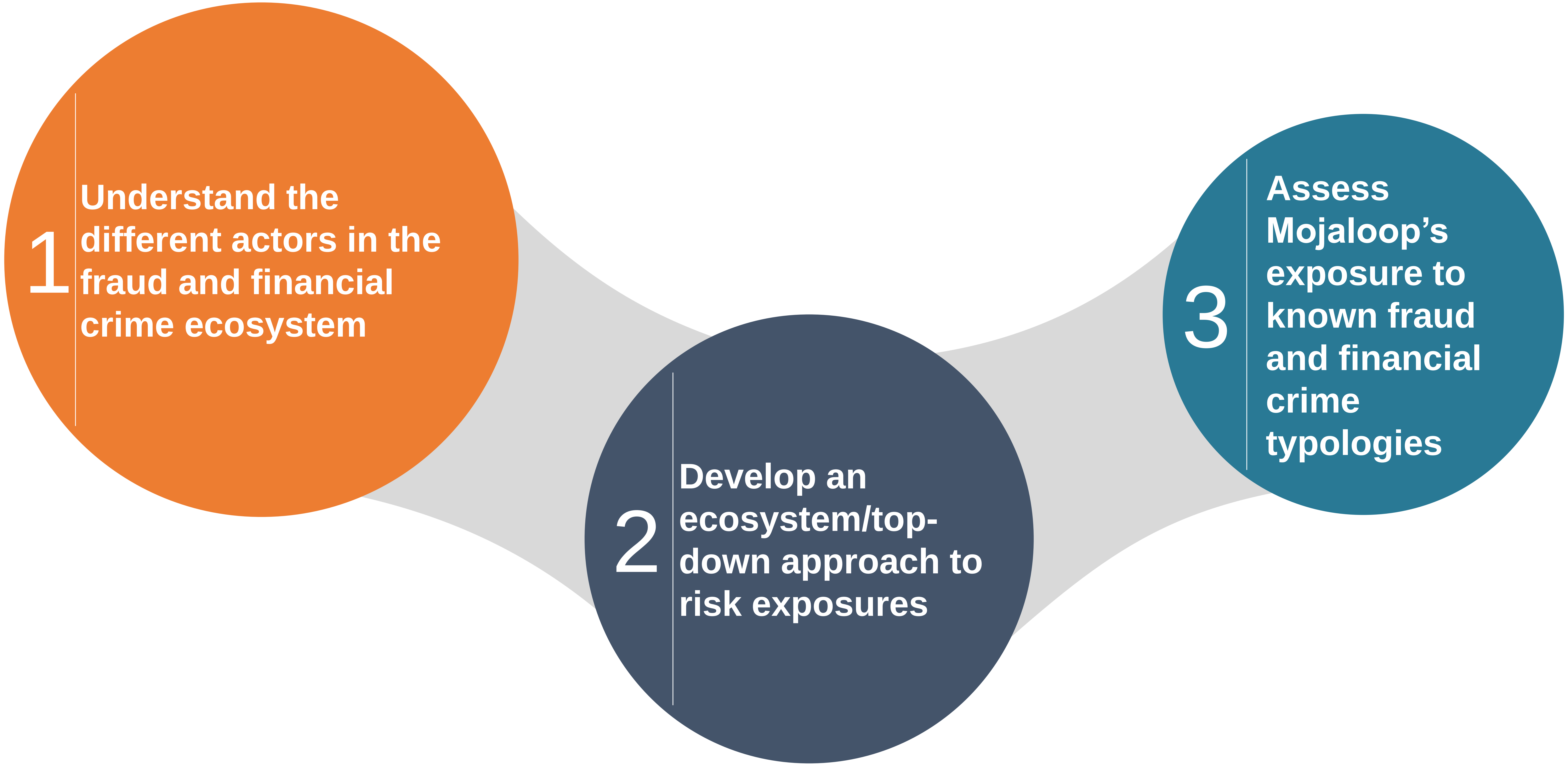
Kenya Police in formation during the Dusit D2 terror attack. FILE



kenya:Banks and mobile money links used to fund Dusit Hotel attack

BY MOBILEMONEYAFRICA - 11 MONTHS AGO

Typologies universe



1 Understand the different actors in the fraud and financial crime ecosystem

2 Develop an ecosystem/top-down approach to risk exposures

3 Assess Mojaloop's exposure to known fraud and financial crime typologies

Typologies Risk Rating Methodology

Approach to Stride and Dread (1/5)

A cross typology approach was utilised for Stride and Dread

(D)READ/(S)TRIDE scoring matrix (Weight/Flag)	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	Test condition
Dread Scoring →						**For a scenario, read each test condition and flag if it is applicable or not**
Stride categorisation ↓						
(S)Spoofing						
W	1	3	2	2	1	Transfer to known tax havens
W	2	1	2	1	1	Dormant account activity
W	2	2	4	1	2	Abnormal hours of transactions
F	3	2	2	1	1	A change of account information or financial instruction with abnormal factors of authentication i.e. Unfamiliar use of Email, SMS or one time pins
(T)Tampering						
F	2	1	1	1	1	Receiving or sending from an account previously flagged as malicious
W	1	0	1	1	0	Identity theft notified to the bank, No account actions performed i.e. ID/Cell phone loss

Typologies Risk Rating Methodology

Approach to Stride and Dread (2/5)

- STRIDE categorises security based threats - A **risk** or issue may only be placed into one of the **S/T/R/I/D/E** elements
- DREAD scores security based threats - A **risk** or issue may be **scored** from **0 to 5** on each of the D/R/E/A/D elements
- A **risk** or issue is placed within a **STRIDE** category and receives a **DREAD** score. Each of the DREAD elements must have a value placed
- To further enhance the outcome of the typology and the appropriate action to be taken on an event each line item was allocated either a flag or weight
- A **flag** line item is determined by an indicator of **compromise**. These are line items that are regarded as severe in nature and carry a weight value
- A **weight** line item is **not** an indicator of **compromise** but an attribute of the scenario that carries some risk. **All** line items **have** a **weight** dependent on the use case
- A risk or issue is dependent of a number of line items given the scope of what is assessed. Each line item may not be an indicator of compromise but may have weight on the scores e.g.

Weight line item:
Access to a user profile was performed during abnormal hours

Flag line item:
Access to a user profile was performed from a malicious foreign state

Typologies Risk Rating Methodology

Approach to Stride and Dread (3/5)

- A score is created for each risk instance/line item
- Example scenario: A client receives a fraudulent SMS from a malicious party whom captures their data

STRIDE Placement **SPOOFING**	Weight	Applicable	**DREAD SCORE N/5** **Damage, Reproducibility, Exploitability, Affected Users and Discoverability**
- False communication	W	✖	D(3), R(2), E(1), A(1), D(2) = 1.8
- Documentation falsified	F		D(1), R(4), E(4), A(2), D(3) = 2.8
TAMPERING			
- Data stolen during capture	F	✖	D(5), R(3), E(5), A(3), D(0) = 4
- Data stolen during processing	F		D(5), R(2), E(5), A(3), D(2) = 3.4
Etc….			**…..**

Score
Flagged Instance; High-risk
31% Spoofing @ 1.8/5.8
69% Tampering @ 4/5.8

(Greatest value)
Damage = (5) Severe
Reproducibility = (3) Moderate
Exploitability = (5) Severe
Affected Users = (3) Moderate
Discoverability = (2) Limited

Typologies Risk Rating Methodology

Approach to Stride and Dread (4/5)

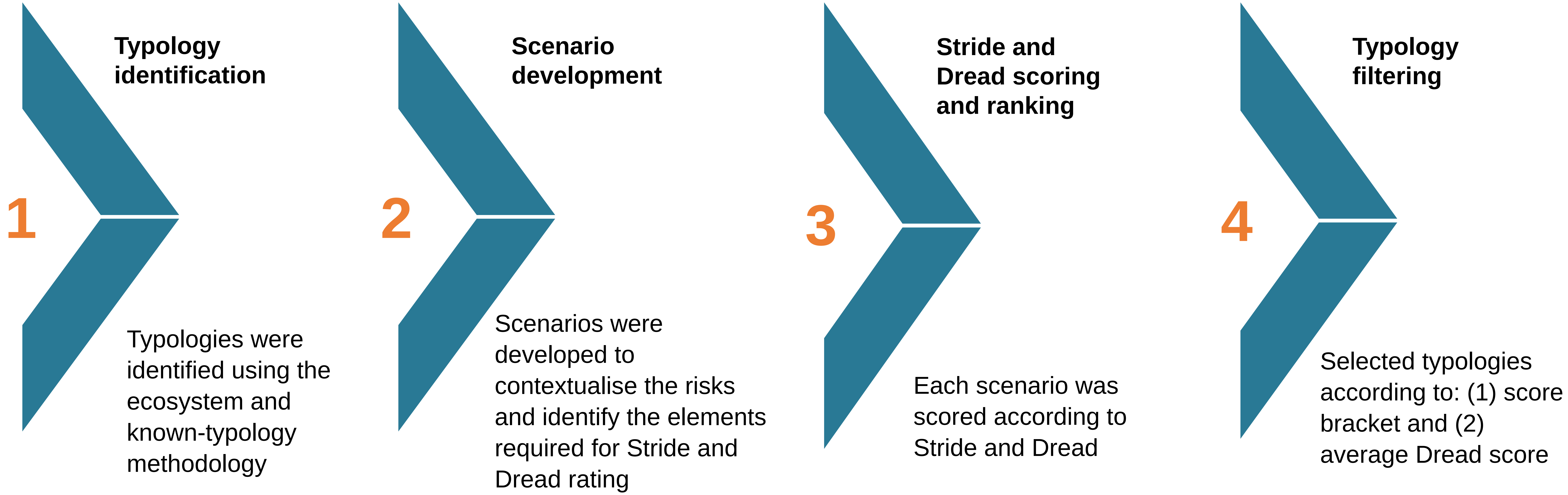
DREAD Table		DREAD Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) /5
Damage	**Dread Score**	**Reputational or financial damage**
	0	No damage to business or client
	1	Limited risk of reputational or financial damage
	2	Low to notable company or client damage
	3	Moderate damage to company or client (Non-news worthy/minor financial damage)
	4	High reputational or financial damage (News worthy/Social media/moderate financial damage)
	5	Critical reputational or financial damage (PR intervention required/high financial damage)
Reproducibility		**A fraudulent action is reproducible before detection.**
	0	No reproducibility, one time action
	1	Limited reproducibility with in a time frame
	2	Low reproducibility, can only be reproduced certain amount before detection
	3	Moderate reproducibility, action can be reproduced and will take time to detect
	4	High reproducibility, repeated action with low chance of detection
	5	Critical reproducibility, repeated action limited to no chance of detection (Manual investigation)
Exploitability		**The ease to circumvent fraud prevention or account access controls**
	0	Not exploitable, prevented by sufficient controls
	1	Limited exploitability, circumvention unlikely
	2	Low exploitability, specific prerequisites required
	3	Moderate exploitability, limited controls for prevention
	4	High exploitability, no visible controls to prevent the action, monitoring in place
	5	Exploitable, no controls to prevent the action, unmonitored

Typologies Risk Rating Methodology

Approach to Stride and Dread (5/5)

DREAD Table		DREAD Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) /5
Affected Users		**Users affected both internally and external from the action source**
	0	No users affected
	1	Limited affected users, limited to a single user
	2	Low, limited to a single user and a known external entity (Bank/Client)
	3	Moderate, single and multiple external entities (Bank/Client)
	4	High, multiple users and external entities (Bank/Client)
	5	Critical, Unknown entities in the transaction chain (Untraceable endpoints)
Discoverability		**Ability to log and monitor a transaction from source to destination**
	0	No discoverability, Unknown source of action, unknown endpoint, no traceability (Anomaly, outage causes ledger discrepancy)
	1	Limited discoverability, Unknown source of action, unknown endpoint, limited traceability (Remote cash deposit)
	2	Low discoverability, known source of payment and unknown endpoint. Limited traceability (ATM withdrawal in foreign nation)
	3	Moderate discoverability, internal and external action, traceable, not monitored (i.e. External nation payment or online purchase)
	4	High discoverability, internal and external action, traceable, not fully monitored (i.e. Money transfer to known entities)
	5	Fully discoverable, action is internal only, traceable from beginning to end, Monitored process (i.e. Internal money transfer)

Key Typologies Selection Process



1

Typology identification

Typologies were identified using the ecosystem and known-typology methodology

2

Scenario development

Scenarios were developed to contextualise the risks and identify the elements required for Stride and Dread rating

3

Stride and Dread scoring and ranking

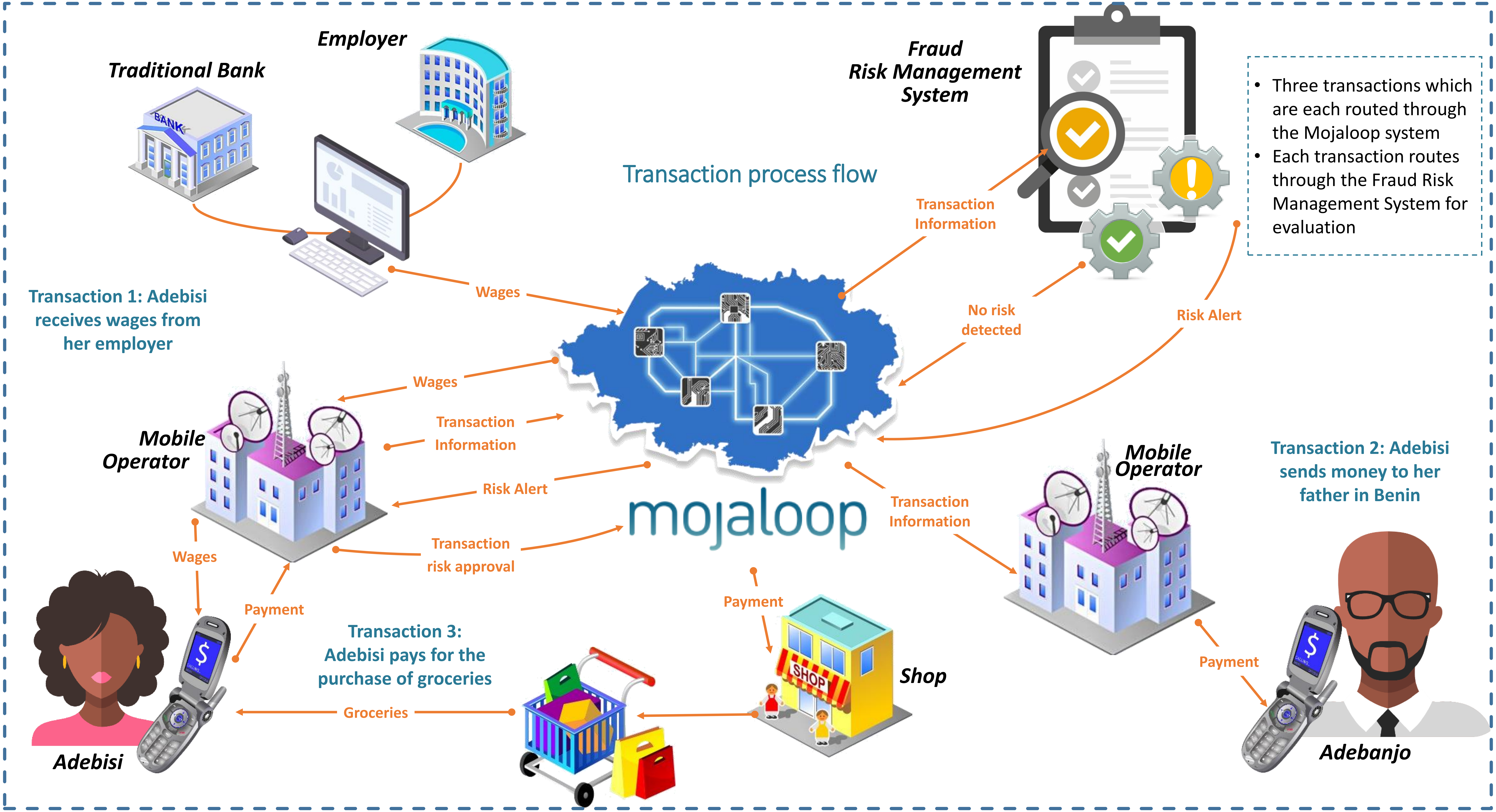
Each scenario was scored according to Stride and Dread

4

Typology filtering

Selected typologies according to: (1) score bracket and (2) average Dread score

Transaction process flow



Traditional Bank

Employer

Fraud Risk Management System

- Three transactions which are each routed through the Mojaloop system
- Each transaction routes through the Fraud Risk Management System for evaluation

Transaction 1: Adebisi receives wages from her employer

Transaction 2: Adebisi sends money to her father in Benin

Transaction 3: Adebisi pays for the purchase of groceries

Wages

Wages

Wages

Transaction Information

Transaction Information

Transaction Information

Risk Alert

Risk Alert

No risk detected

Transaction risk approval

Payment

Payment

Payment

Groceries

mojaloop

Mobile Operator

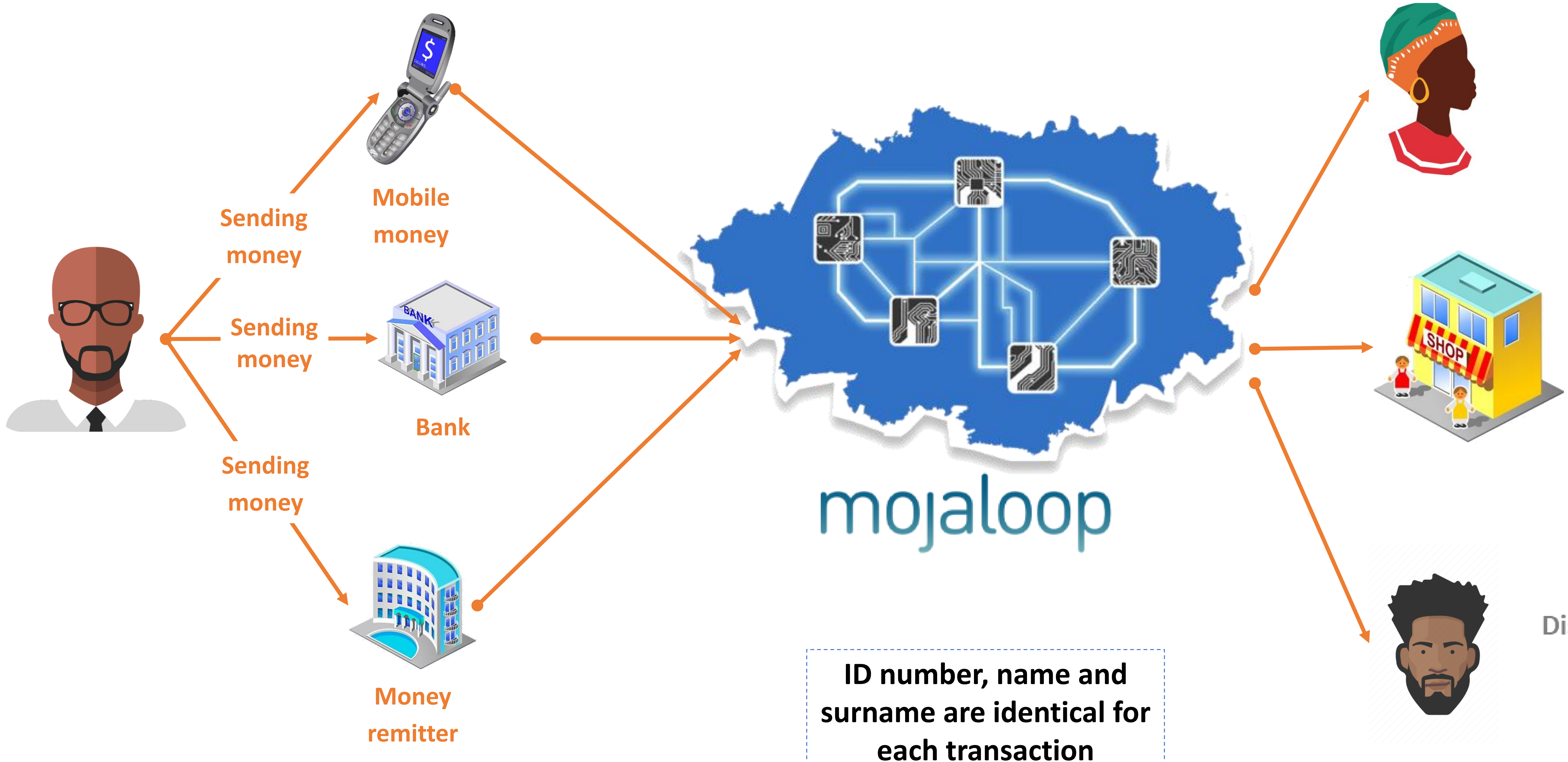
Mobile Operator

Shop

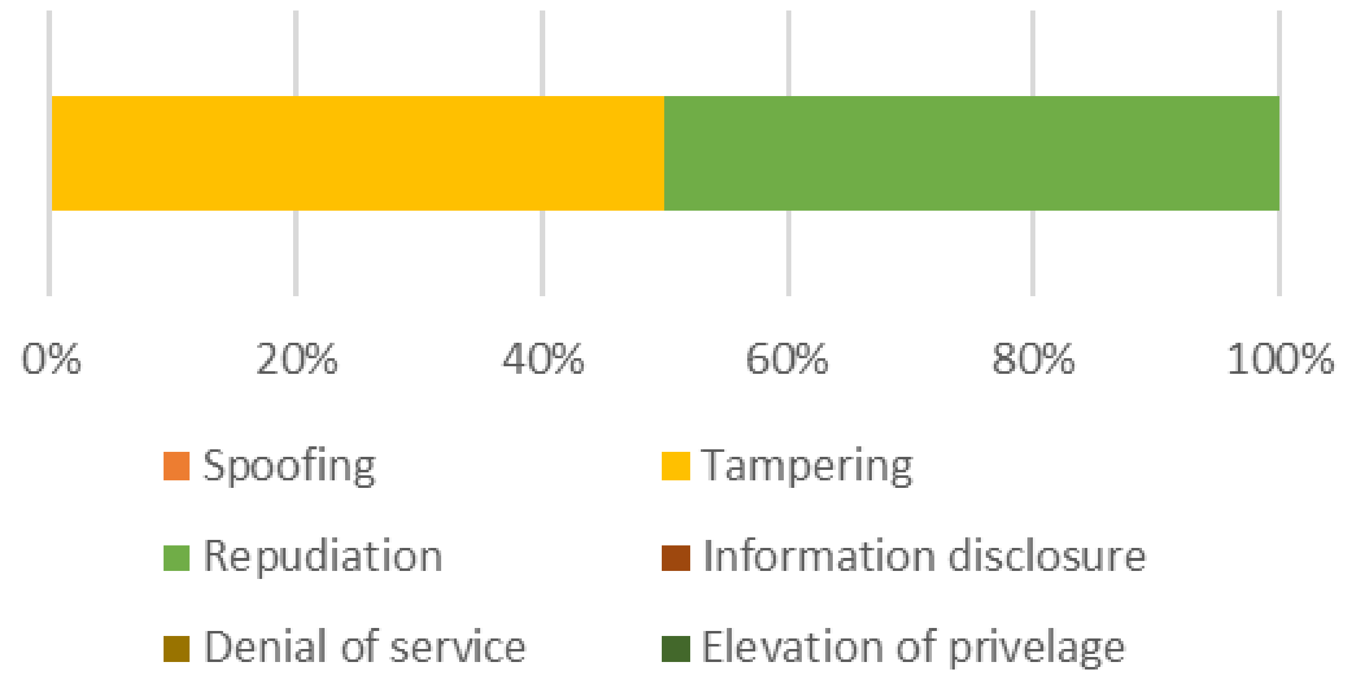
Adebisi

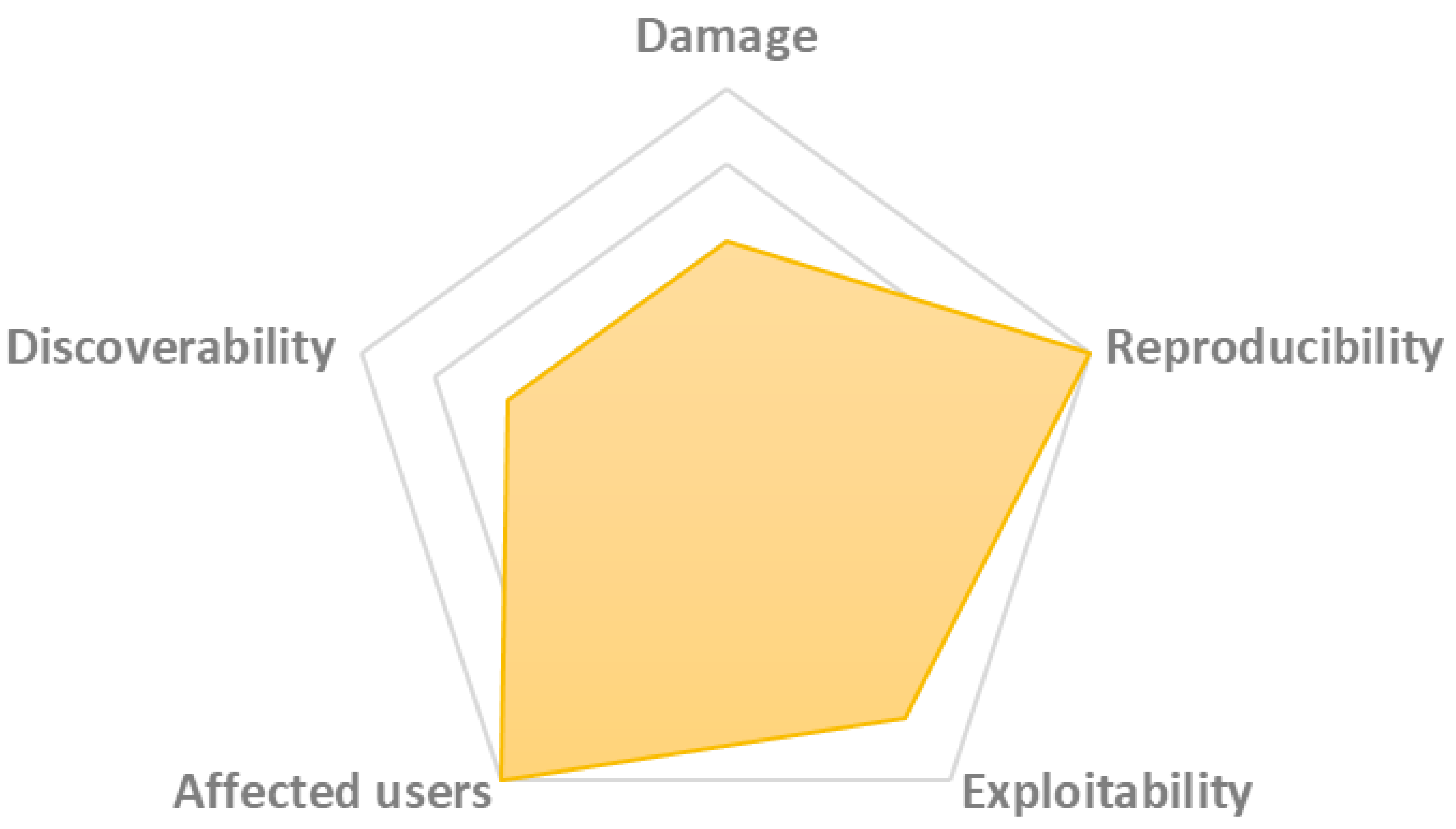
Adebanjo

Review of Selected Typologies #1



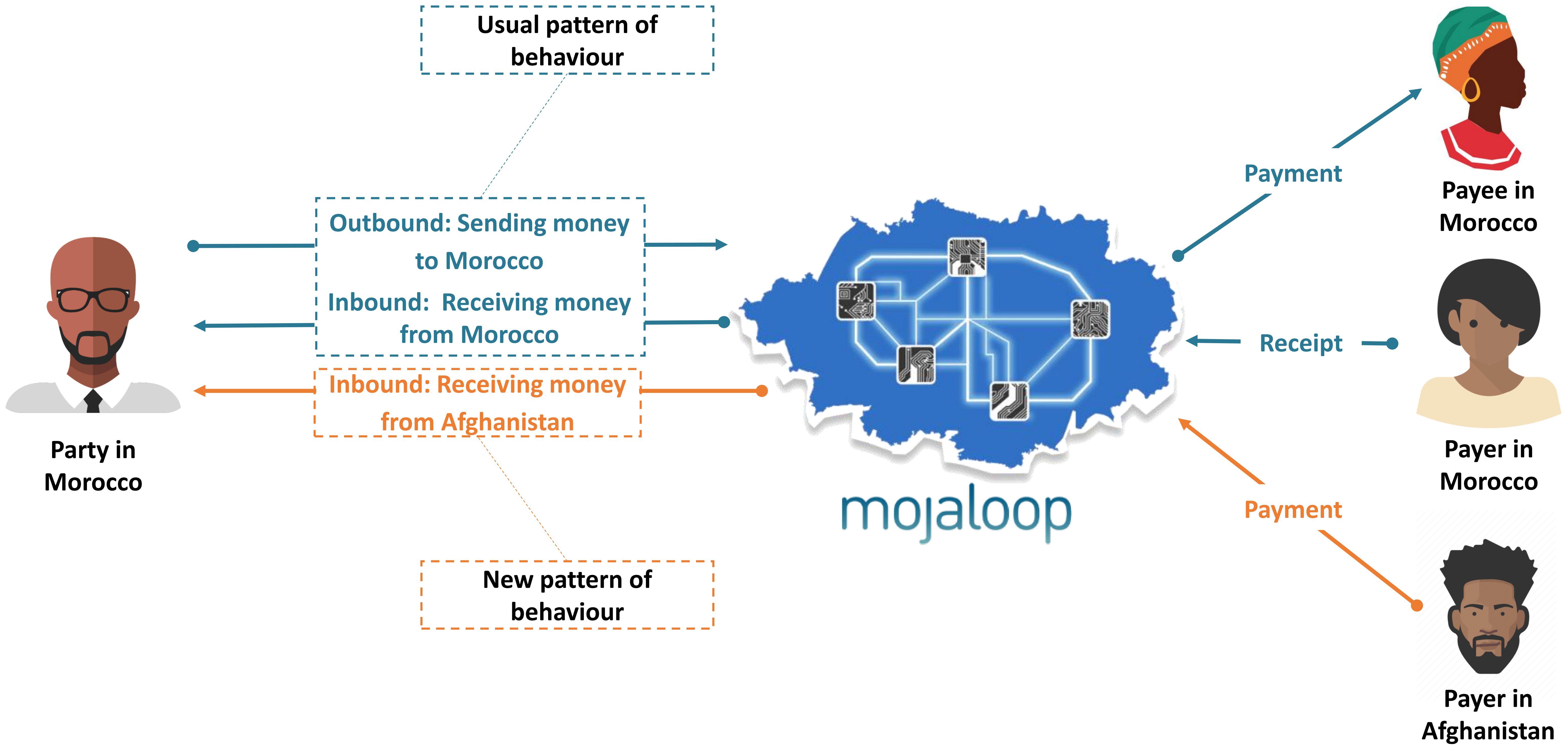
ID number, name and surname are identical for each transaction





POC Demo of typology 1

Review of Selected Typologies #2



Usual pattern of behaviour

Outbound: Sending money to Morocco

Inbound: Receiving money from Morocco

Inbound: Receiving money from Afghanistan

New pattern of behaviour

Party in Morocco

Payment

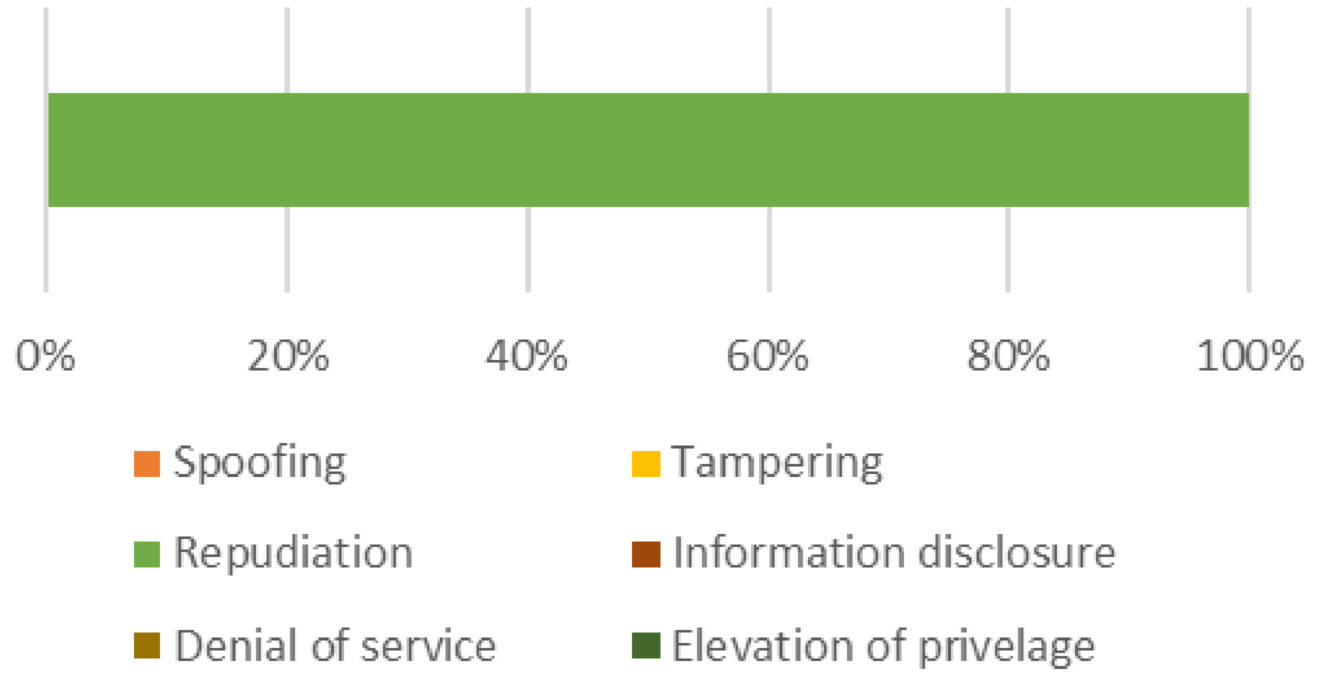
Receipt

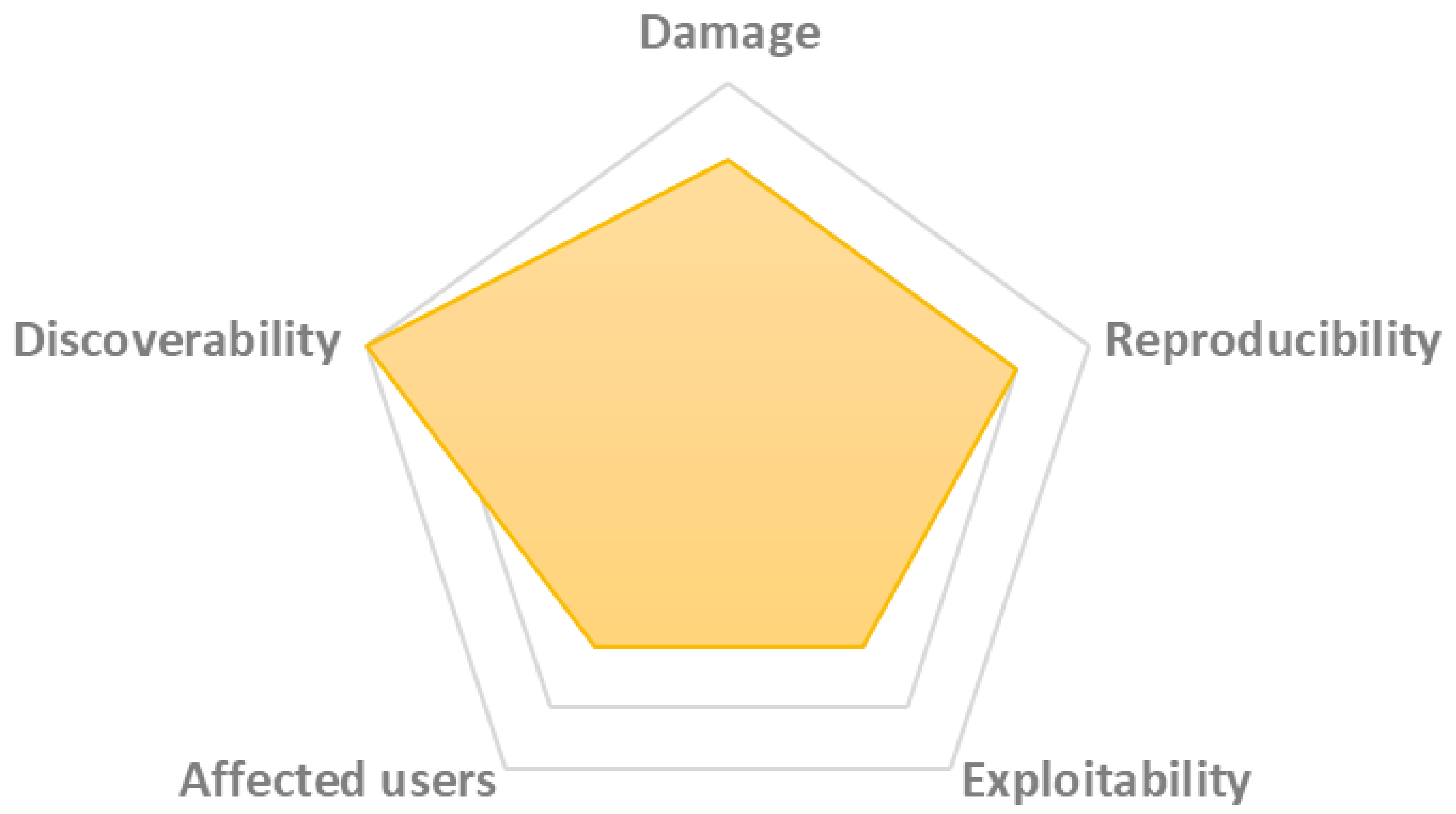
Payment

Payee in Morocco

Payer in Morocco

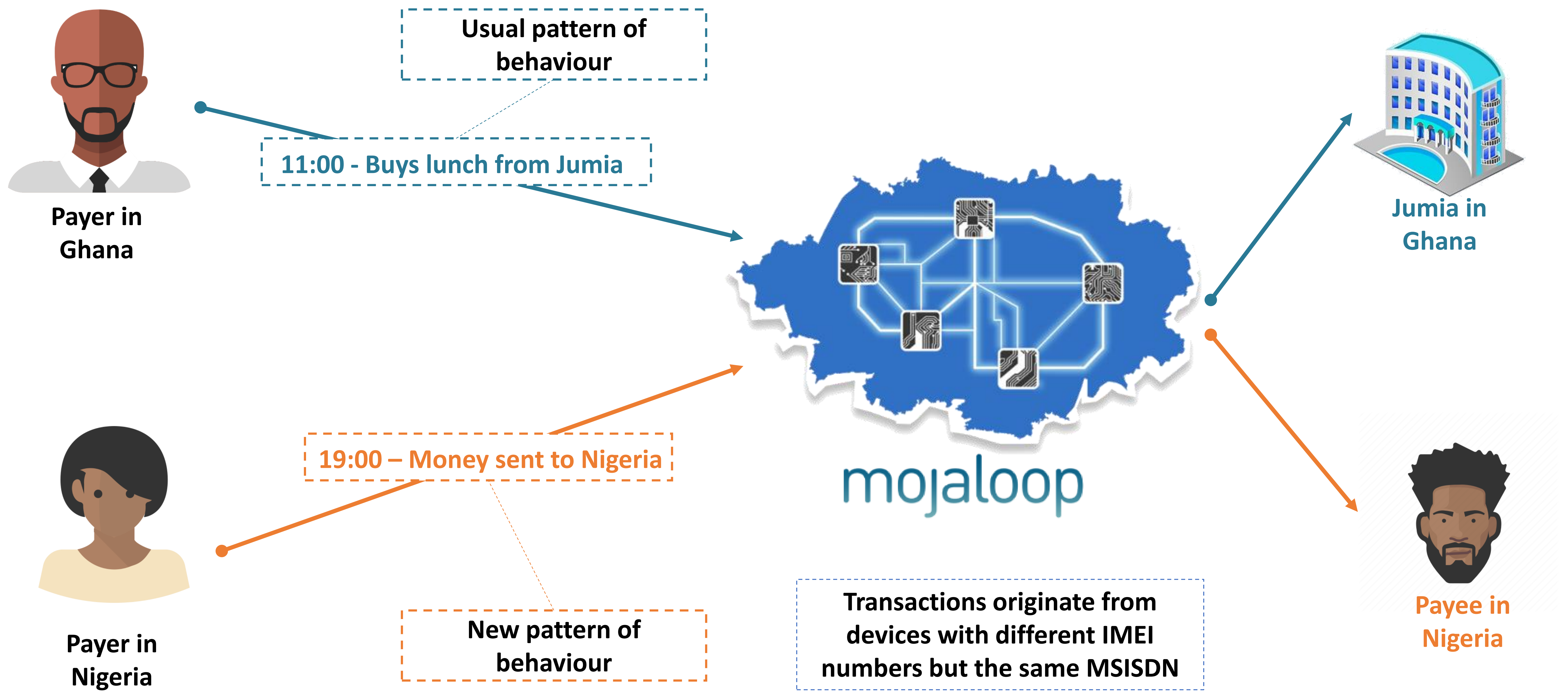
Payer in Afghanistan





POC Demo of typology 2

Review of Selected Typologies #3



Payer in Ghana

Usual pattern of behaviour

11:00 - Buys lunch from Jumia

Payer in Nigeria

19:00 – Money sent to Nigeria

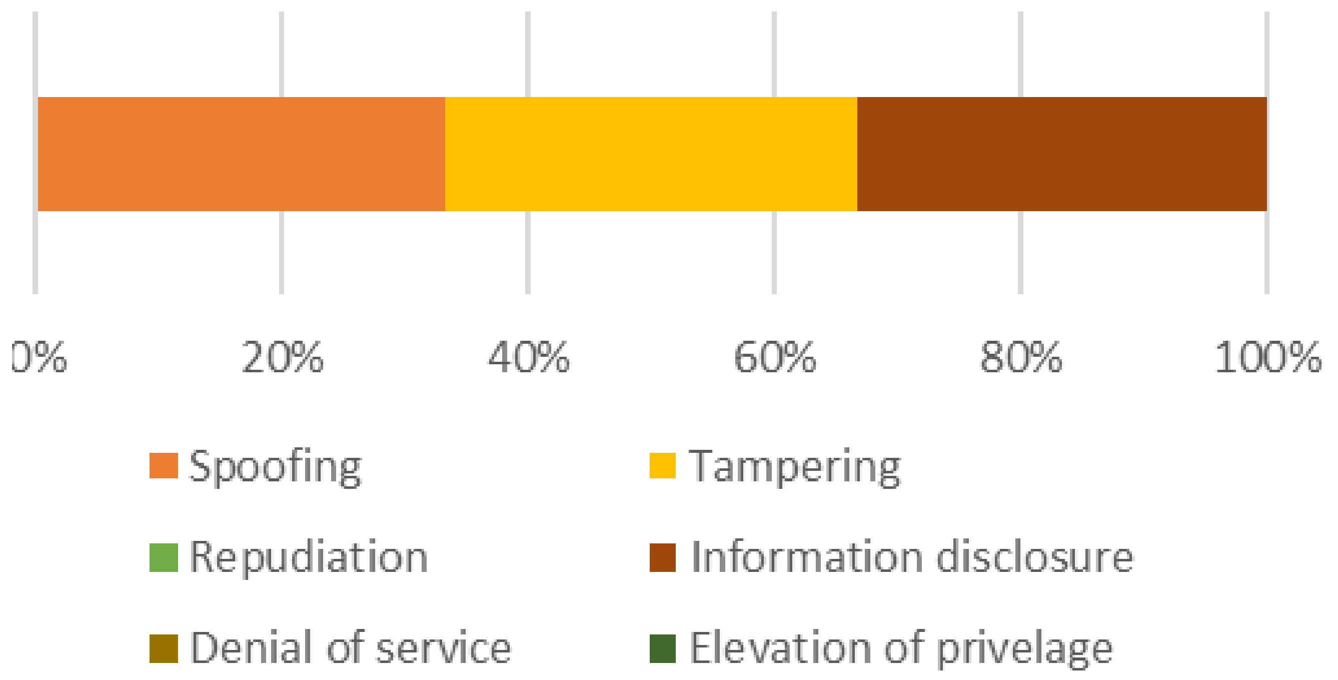
New pattern of behaviour

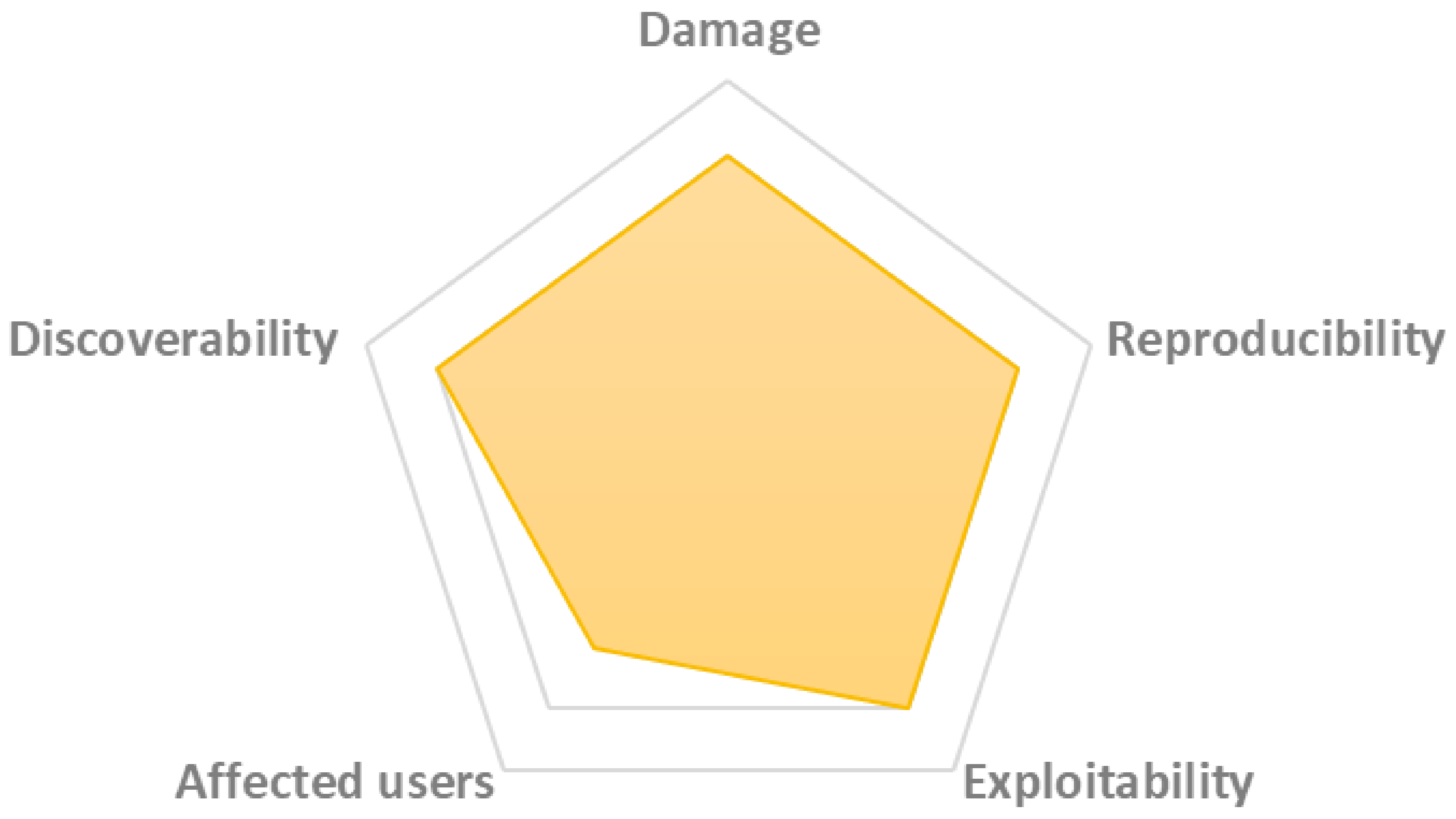
mojaloop

Transactions originate from devices with different IMEI numbers but the same MSISDN

Jumia in Ghana

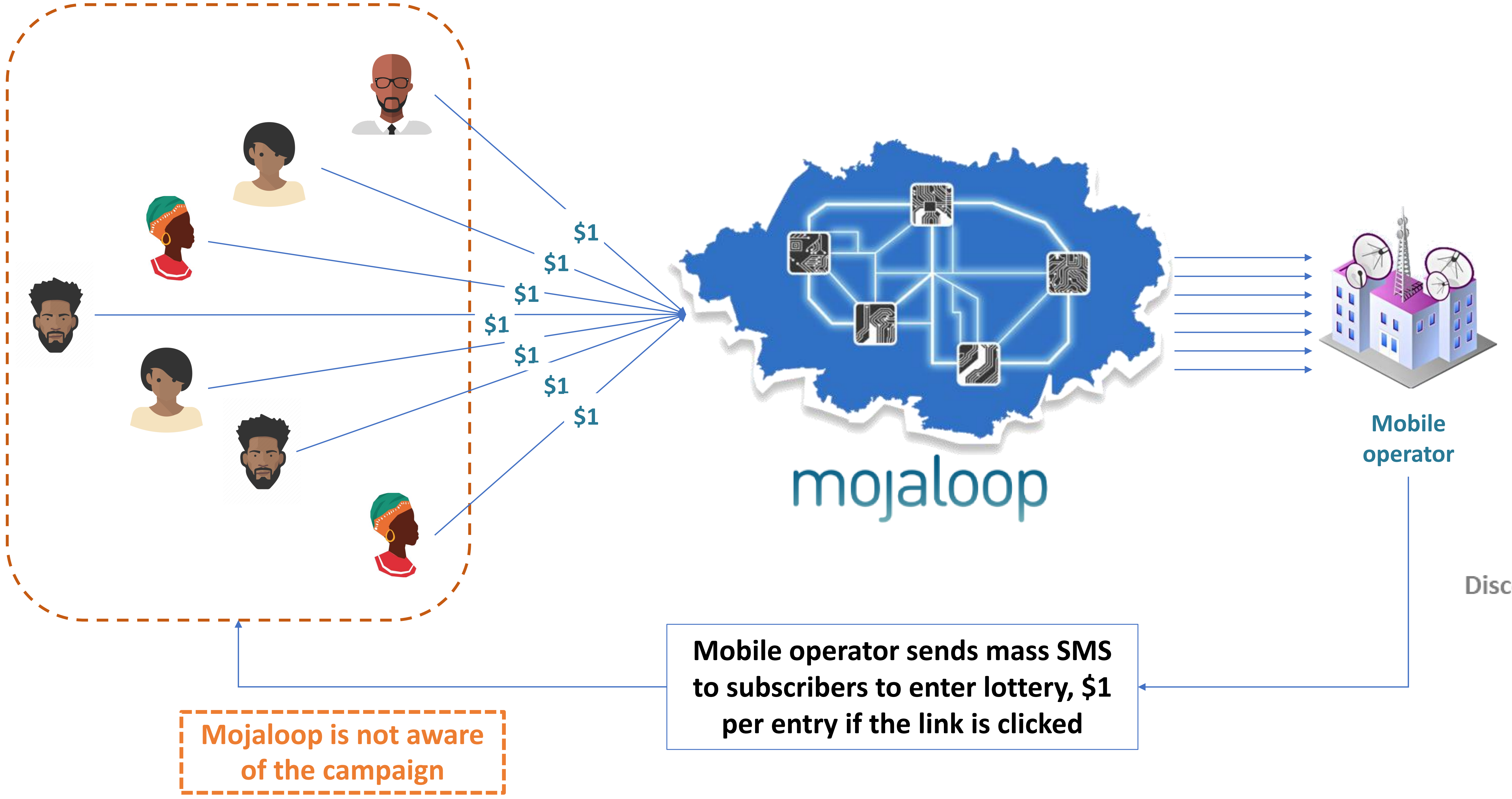
Payee in Nigeria





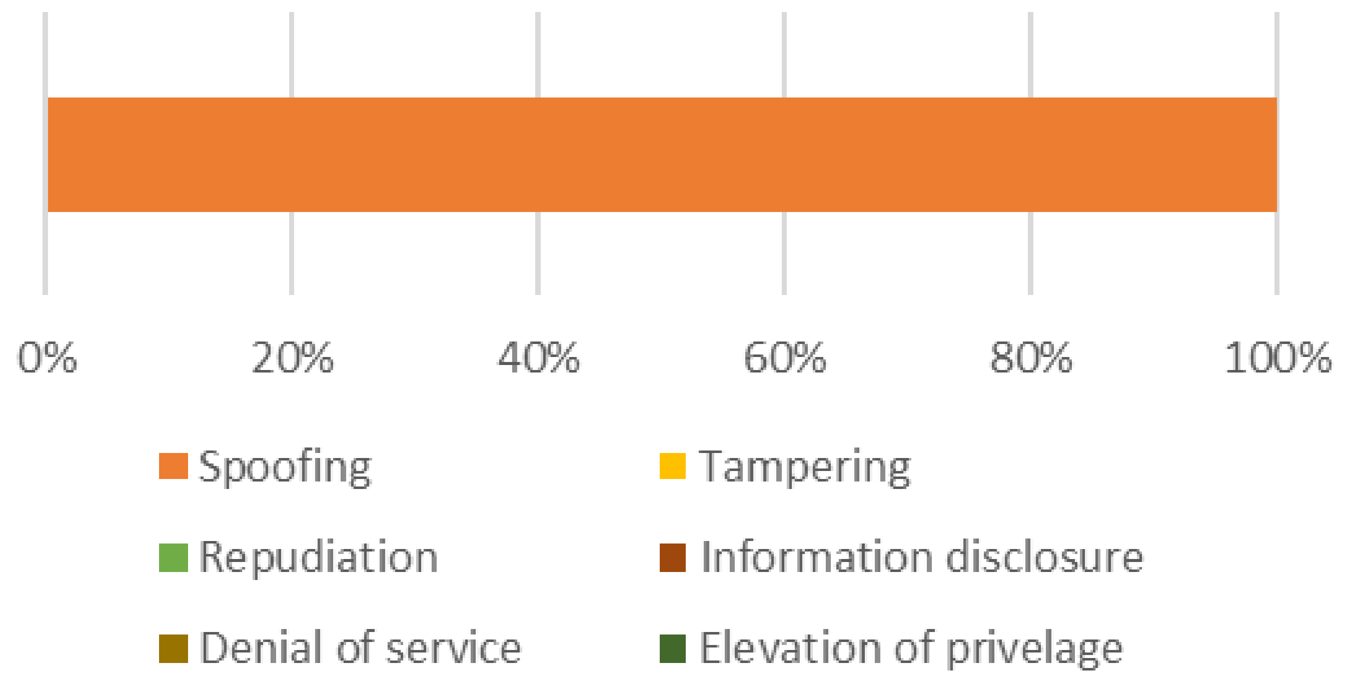
POC Demo of typology 3

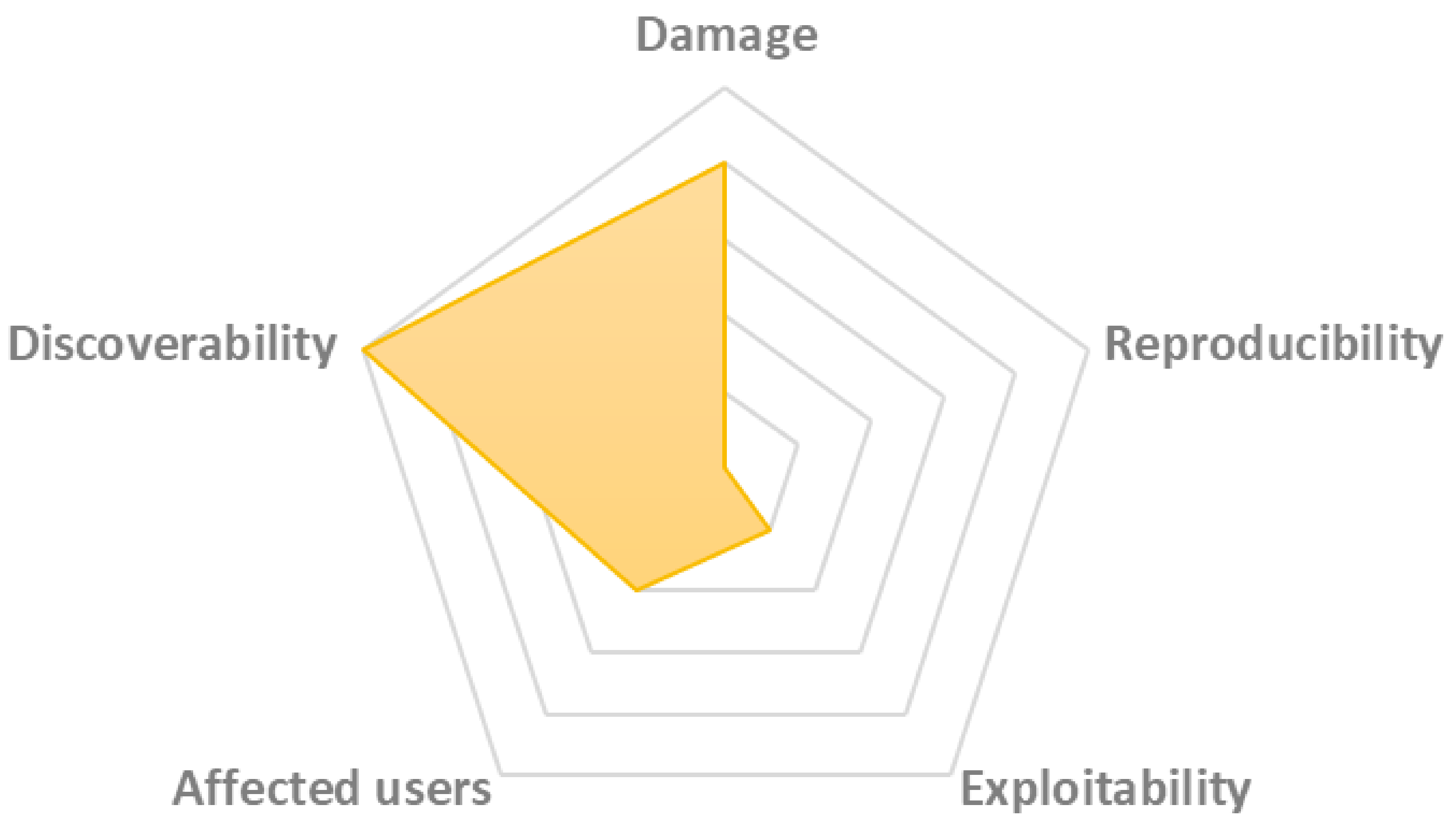
Review of Selected Typologies #4



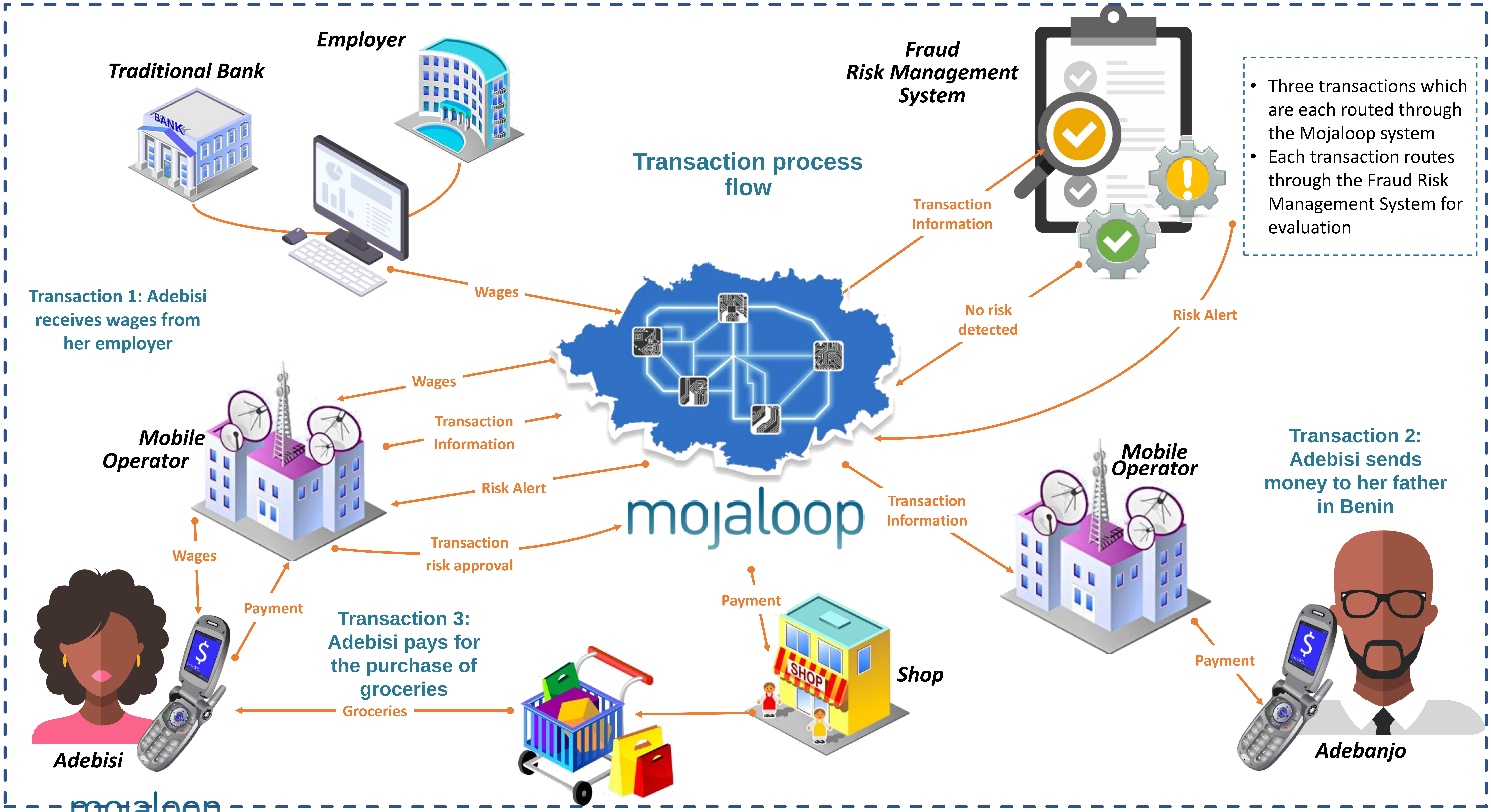
Mobile operator sends mass SMS to subscribers to enter lottery, $1 per entry if the link is clicked

Mojaloop is not aware of the campaign





Transaction process flow



- Three transactions which are each routed through the Mojaloop system
- Each transaction routes through the Fraud Risk Management System for evaluation

Transaction 1: Adebisi receives wages from her employer

Transaction 2: Adebisi sends money to her father in Benin

Transaction 3: Adebisi pays for the purchase of groceries

User requirements

Three major classes of users

Mojaloop Administrator

The Mojaloop Administrator defines one or more users who will interact with the Mojaloop FRMS on behalf of the Mojaloop operator that is hosting the Mojaloop platform

DFSP System (API)

The bulk of the interaction between the DFSP and the Mojaloop platform is anticipated to be through RESTful API hosted on the Mojaloop platform and accessed securely from the DFSP front-end systems

DFSP User

These are employees of the DFSP who would perform risk management functions in response to receiving a risk alert from the FRMS

User requirements

Mojaloop Operator Administrator functions (1/3)

Typology Management

- Create new typologies
- Update existing typologies
- Activate/Deactivate typologies

User requirements

Mojaloop Operator Administrator functions (2/3)

Individual Privacy Rights Management

Individual Privacy Right	Use Case
Right of access	Provide access report
Right to be forgotten	Purge personal information
Right to rectification	Update personal information
Right to object to processing	Limit processing of personal information
Right to restrict processing	
Right to portability	Export personal information
Right to safeguards from automated decision-making and profiling	Review automated risk decision

User requirements

Mojaloop Operator Administrator functions (3/3)

Risk Alert/Case Management

- Escalations
- Investigations
- Rules auditing and tracing
- Overrides and remediation

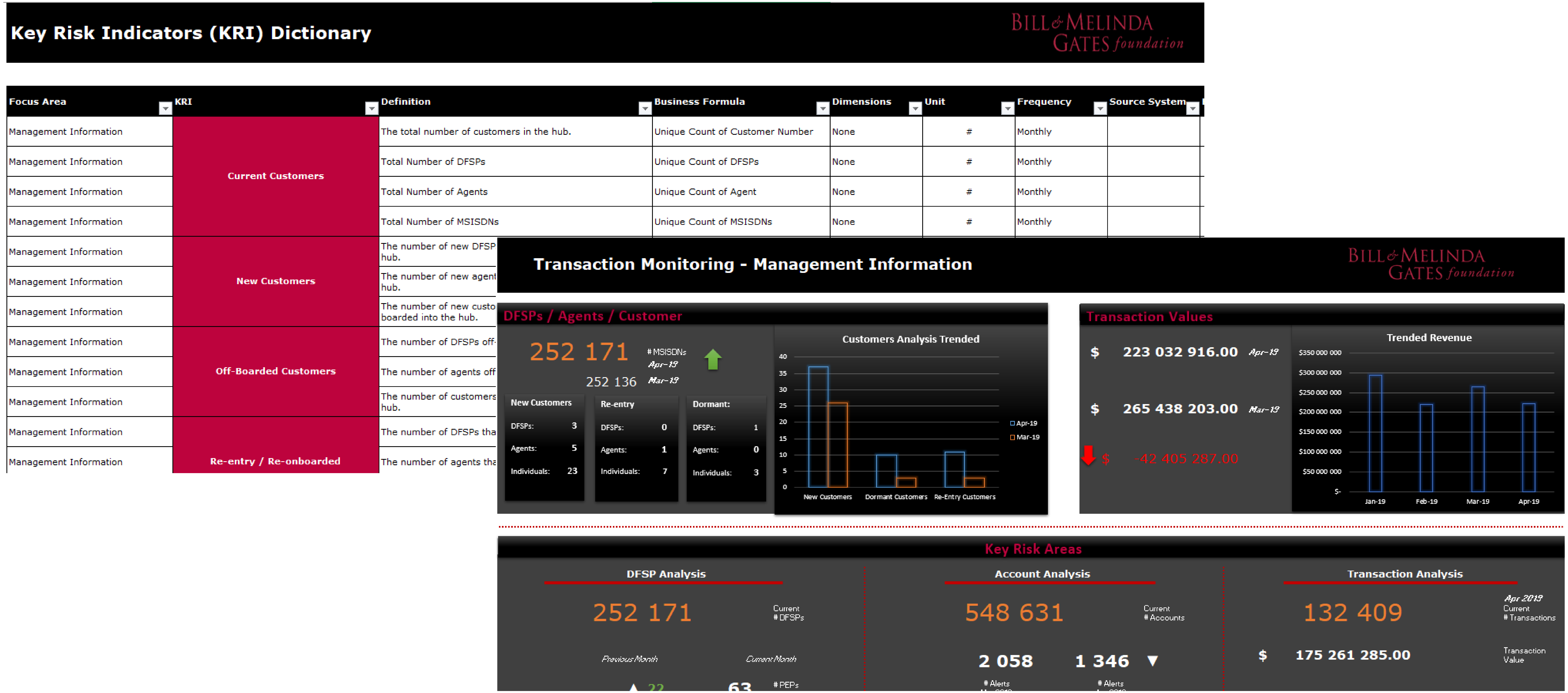
Data Management

- Identify data quality issues
- Data remediation

Reporting

- DFSP Service Level Agreement performance monitoring
- Transaction Monitoring Management Information

Key Risk Indicator (KRI) dashboard



Key Risk Indicators (KRI) Dictionary

BILL & MELINDA GATES foundation

Focus Area	KRI	Definition	Business Formula	Dimensions	Unit	Frequency	Source System
Management Information	Current Customers	The total number of customers in the hub.	Unique Count of Customer Number	None	#	Monthly	
Management Information		Total Number of DFSPs	Unique Count of DFSPs	None	#	Monthly	
Management Information		Total Number of Agents	Unique Count of Agent	None	#	Monthly	
Management Information		Total Number of MSISDNs	Unique Count of MSISDNs	None	#	Monthly	
Management Information	New Customers	The number of new DFSP hub.					
Management Information		The number of new agent hub.					
Management Information		The number of new custo boarded into the hub.					
Management Information	Off-Boarded Customers	The number of DFSPs off-					
Management Information		The number of agents off					
Management Information		The number of customers hub.					
Management Information	Re-entry / Re-onboarded	The number of DFSPs tha					
Management Information		The number of agents tha					

Transaction Monitoring - Management Information

BILL & MELINDA GATES foundation

DFSPs / Agents / Customer

252 171 # MSISDNs Apr-19

252 136 Mar-19

New Customers		Re-entry		Dormant:	
DFSPs:	3	DFSPs:	0	DFSPs:	1
Agents:	5	Agents:	1	Agents:	0
Individuals:	23	Individuals:	7	Individuals:	3

Transaction Values

$ 223 032 916.00 Apr-19

$ 265 438 203.00 Mar-19

$ -42 405 287.00

Key Risk Areas

DFSP Analysis

252 171 Current # DFSPs

Previous Month Current Month

▲ 22 63 # PEPs

Account Analysis

548 631 Current # Accounts

2 058 1 346 ▼

Alerts # Alerts

Transaction Analysis

132 409 Apr 2019 Current # Transactions

$ 175 261 285.00 Transaction Value

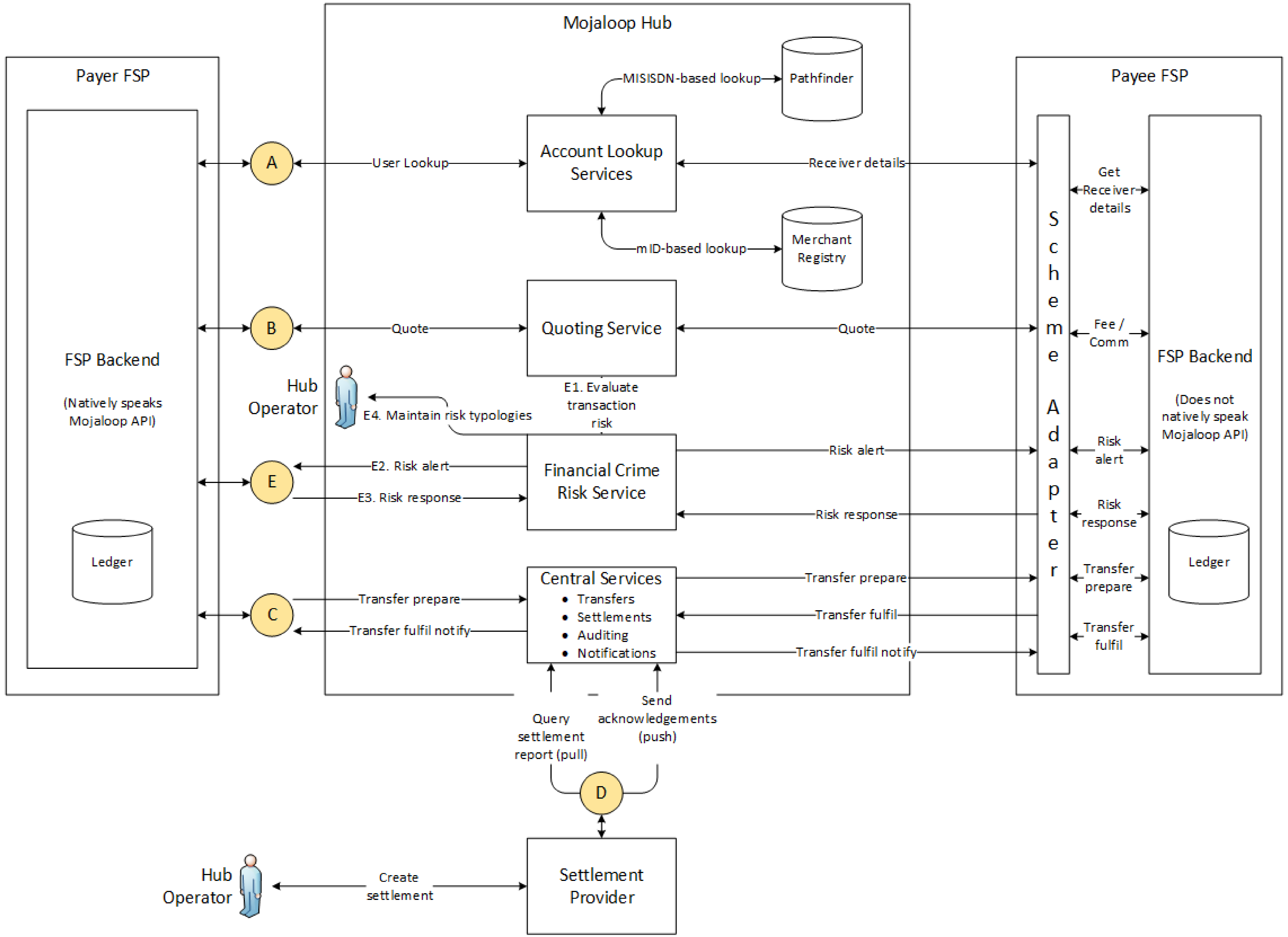
User requirements

Digital Financial Service Provider functions

RESTful APIs

- Receive fraud risk alert
- Resolve fraud risk alert
- Escalate fraud risk alert

DFSP front-end required



Mojaloop Hub

Payer FSP

FSP Backend

(Natively speaks Mojaloop API)

Ledger

A

B

E

C

D

User Lookup

MISISDN-based lookup

Pathfinder

Account Lookup Services

mID-based lookup

Merchant Registry

Quote

Quoting Service

Hub Operator

E4. Maintain risk typologies

E1. Evaluate transaction risk

E2. Risk alert

E3. Risk response

Financial Crime Risk Service

Transfer prepare

Transfer fulfil notify

Central Services

- Transfers
- Settlements
- Auditing
- Notifications

Query settlement report (pull)

Send acknowledgements (push)

Hub Operator

Create settlement

Settlement Provider

Receiver details

Quote

Risk alert

Risk response

Transfer prepare

Transfer fulfil

Transfer fulfil notify

Payee FSP

Scheme Adapter

Get Receiver details

Fee / Comm

Risk alert

Risk response

Transfer prepare

Transfer fulfil

FSP Backend

(Does not natively speak Mojaloop API)

Ledger

mojaloop

User requirements

DFSP User functions

Alert Management

- List outstanding cases
- Access case
- Review alert
- Clear alert
- Reject transfer
- Refer/Escalate/Query case
- Review case history

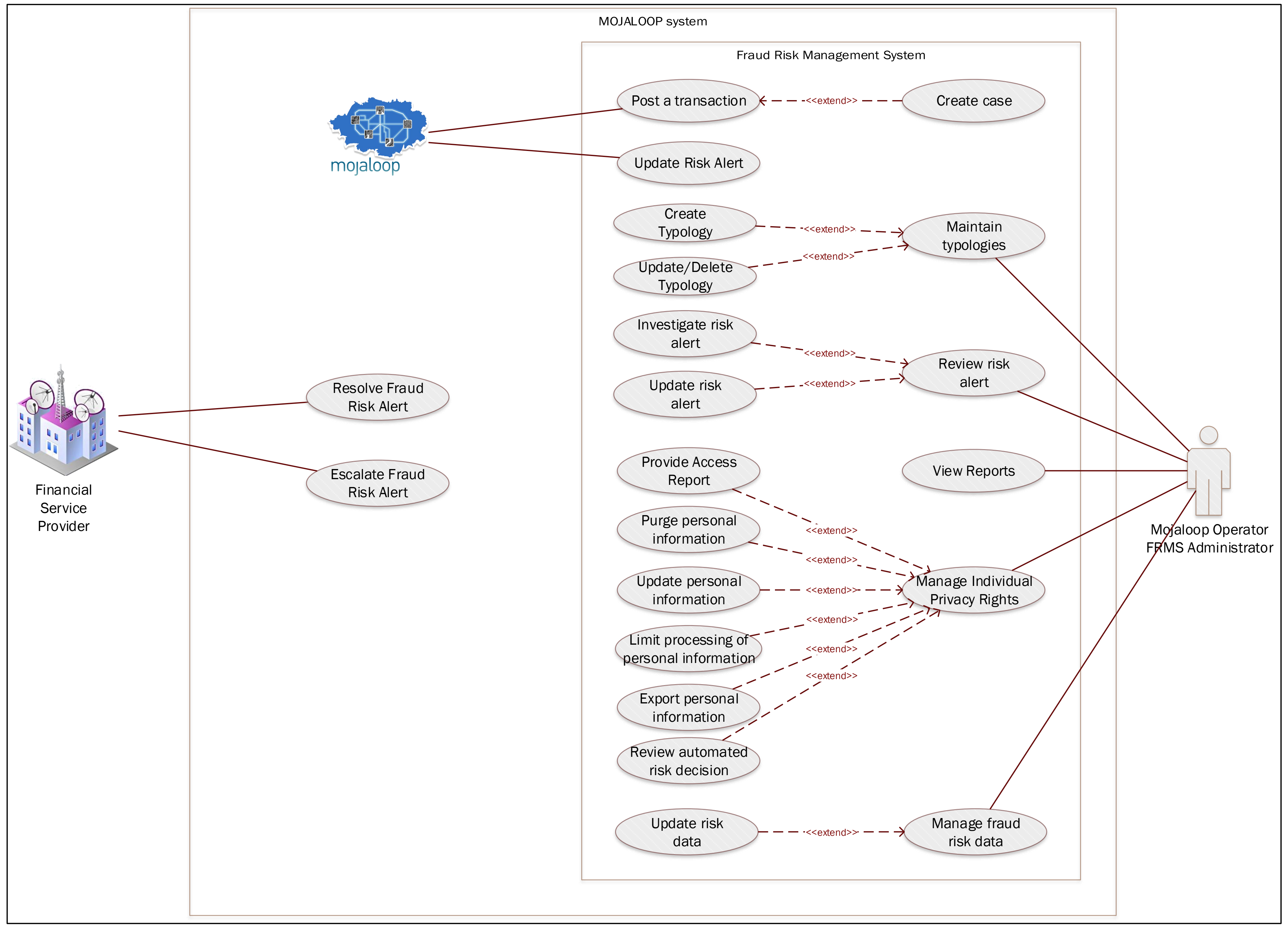
BRD Preview

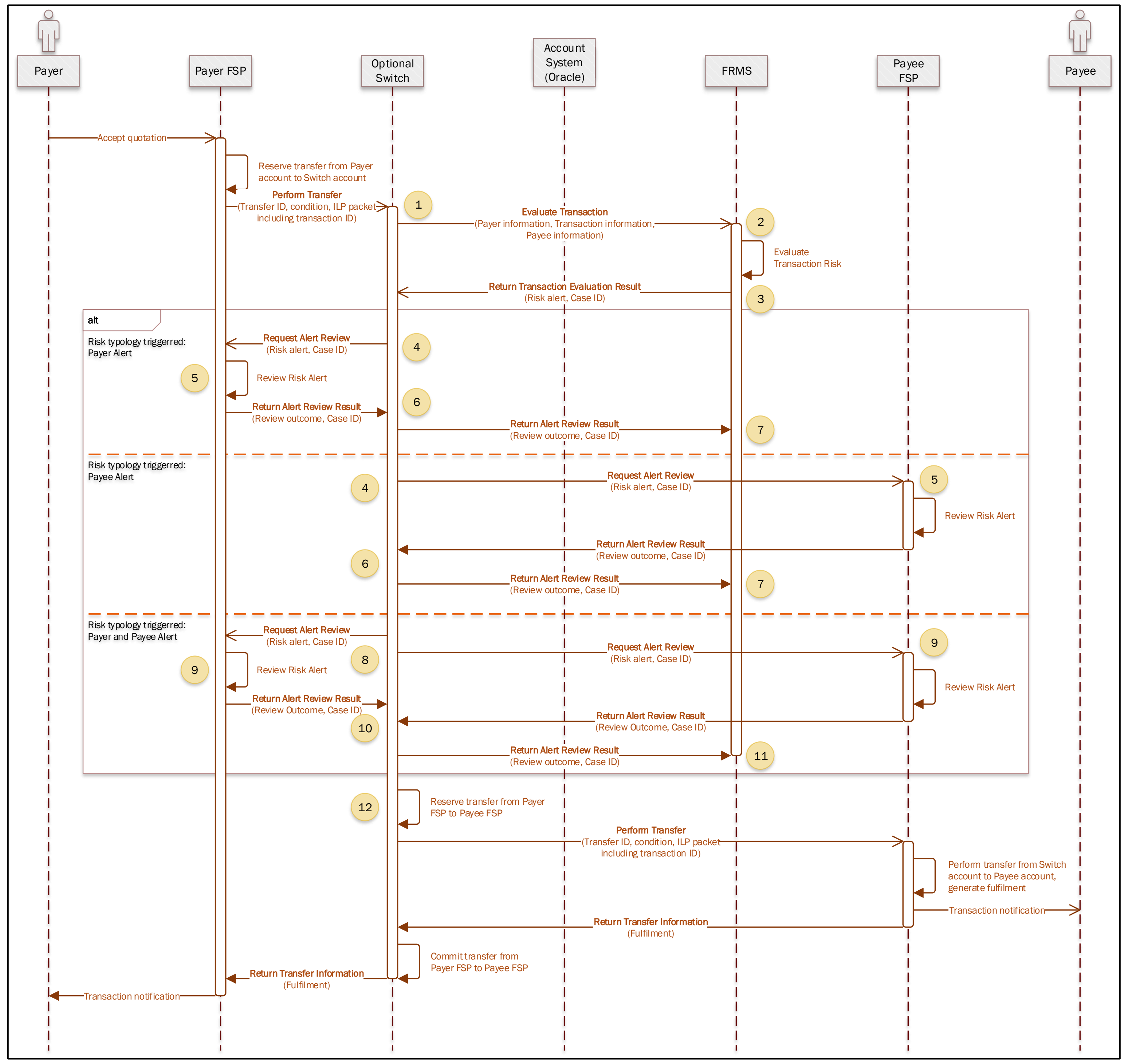
Detail the business requirements for the design of an integrated Fraud Risk Management Framework to complement the Mojaloop software

Gain agreement with stakeholders about the business requirements

Align the business strategy, the business processes and the business requirements

Provide a foundation to solution design, development and implementation of a solution

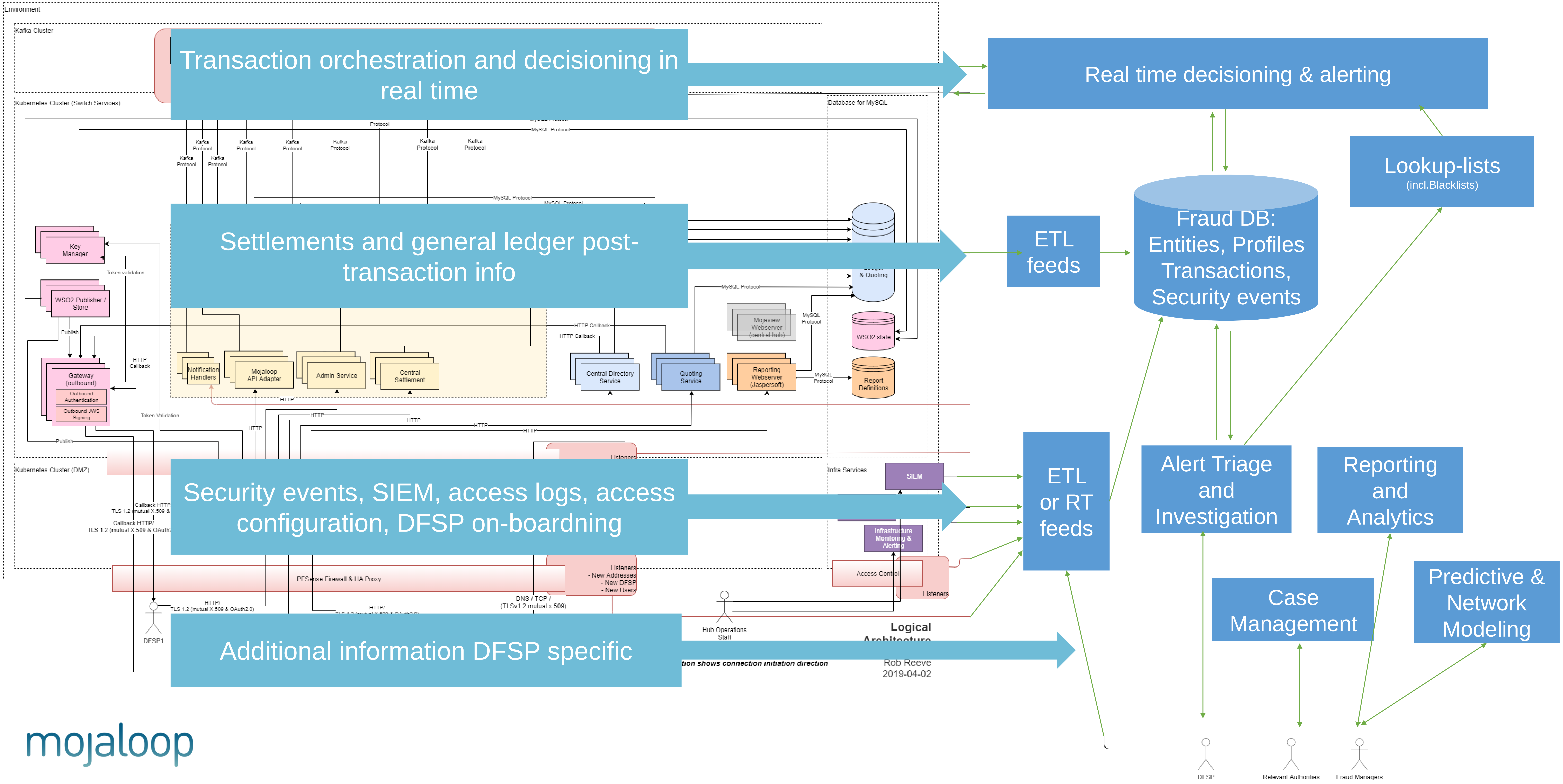



Payer
Payer FSP
Optional Switch
Account System (Oracle)
FRMS
Payee FSP
Payee
Accept quotation
Reserve transfer from Payer account to Switch account
Perform Transfer
(Transfer ID, condition, ILP packet including transaction ID)
1
Evaluate Transaction
(Payer information, Transaction information, Payee information)
2
Evaluate Transaction Risk
Return Transaction Evaluation Result
(Risk alert, Case ID)
3
alt
Risk typology triggerred: Payer Alert
Request Alert Review
(Risk alert, Case ID)
4
5
Review Risk Alert
Return Alert Review Result
(Review outcome, Case ID)
6
Return Alert Review Result
(Review outcome, Case ID)
7
Risk typology triggerred: Payee Alert
Request Alert Review
(Risk alert, Case ID)
4
5
Review Risk Alert
Return Alert Review Result
(Review outcome, Case ID)
6
Return Alert Review Result
(Review outcome, Case ID)
7
Risk typology triggerred: Payer and Payee Alert
Request Alert Review
(Risk alert, Case ID)
8
Request Alert Review
(Risk alert, Case ID)
9
9
Review Risk Alert
Review Risk Alert
Return Alert Review Result
(Review Outcome, Case ID)
10
Return Alert Review Result
(Review Outcome, Case ID)
Return Alert Review Result
(Review outcome, Case ID)
11
12
Reserve transfer from Payer FSP to Payee FSP
Perform Transfer
(Transfer ID, condition, ILP packet including transaction ID)
Perform transfer from Switch account to Payee account, generate fulfilment
Transaction notification
Return Transfer Information
(Fulfilment)
Commit transfer from Payer FSP to Payee FSP
Return Transfer Information
(Fulfilment)
Transaction notification

mojaloop

Architecture and integration considerations

Our understanding of Mojaloop integration requirements



Transaction orchestration and decisioning in real time

Settlements and general ledger post-transaction info

Security events, SIEM, access logs, access configuration, DFSP on-boarding

Additional information DFSP specific

Real time decisioning & alerting

Lookup-lists (incl.Blacklists)

ETL feeds

Fraud DB: Entities, Profiles Transactions, Security events

ETL or RT feeds

Alert Triage and Investigation

Reporting and Analytics

Case Management

Predictive & Network Modeling

What are the next steps?

Breakout session with community

Feedback and comments from community

Final review of deliverables

Community to plan, prioritise and build

Q&A