FRMS
CoE

OSS FRMS SOLUTION

“Actio”: Open-Source Transaction Monitoring System

July 27, 2022

ANNOUNCEMENTS

- My last day at Sybrin is Friday
- The Bill & Melinda Gates Foundation created
  - The Fraud Risk Management Systems Center of Excellence (FRMS CoE)
  - Greg McCormick, Executive Director of the FRMS CoE – no I wasn't poached
    - Still plan to be involved with the Mojaloop Community and Mojaloop CBDC Center of Excellence in Singapore
- Sybrin Team
  - Roland Van Hee – CTO, Technical Governing Board
    - Jason Damanovich - CIO and BU head for Open-Source Initiative including Mojaloop
      - Johannes Foley – DA Member and Product Manager, Mojaloop and Fraud Risk Management
    - Salvatore Errera - BU Head: Innovations and Product | Innovations, Product Manager Onboarding and Biometrics, Business Interface for "Actio" FRMS TMS
- MVP for FRMS system of "Actio" complete

Let's Recap

A GROUP OF USERS PERFORM ACTIONS

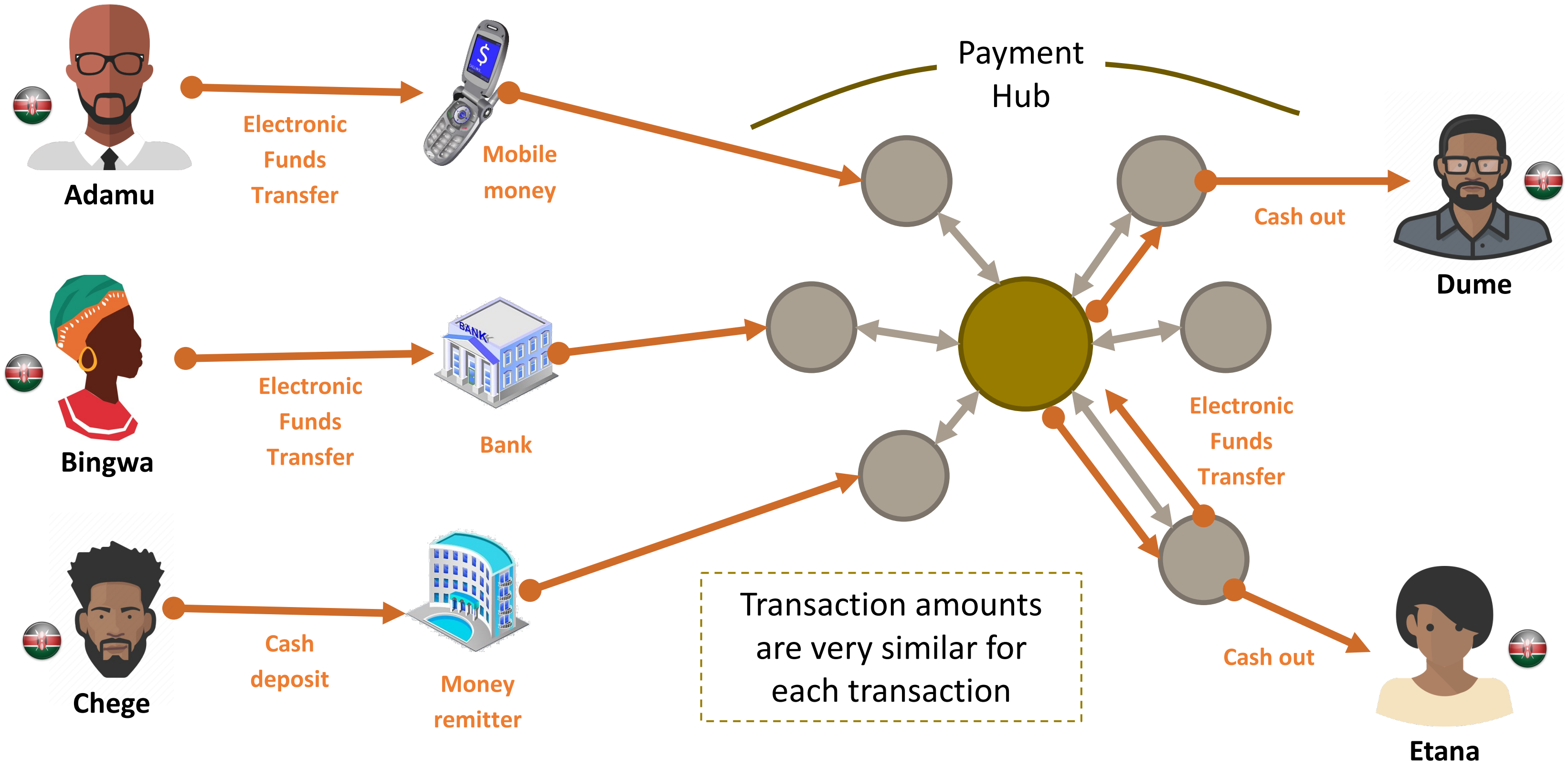
Users act, rules are assessed, and you look for patterns of fraud, or typologies.

Adamu, Bingwa and Chege were convinced by Etana that they'd won a prize and needed to pay a small administration fee to Etana to process their winnings.

They each transfer the money to Etana's account.

As each payment arrives, Etana immediately cashes out the payment. Adamu's payment arrives after the money agent has closed for the day and Etana immediately transfer his payment to her associate, Dume.

Dume cashes out the payment first thing the next morning.



Transaction amounts are very similar for each transaction

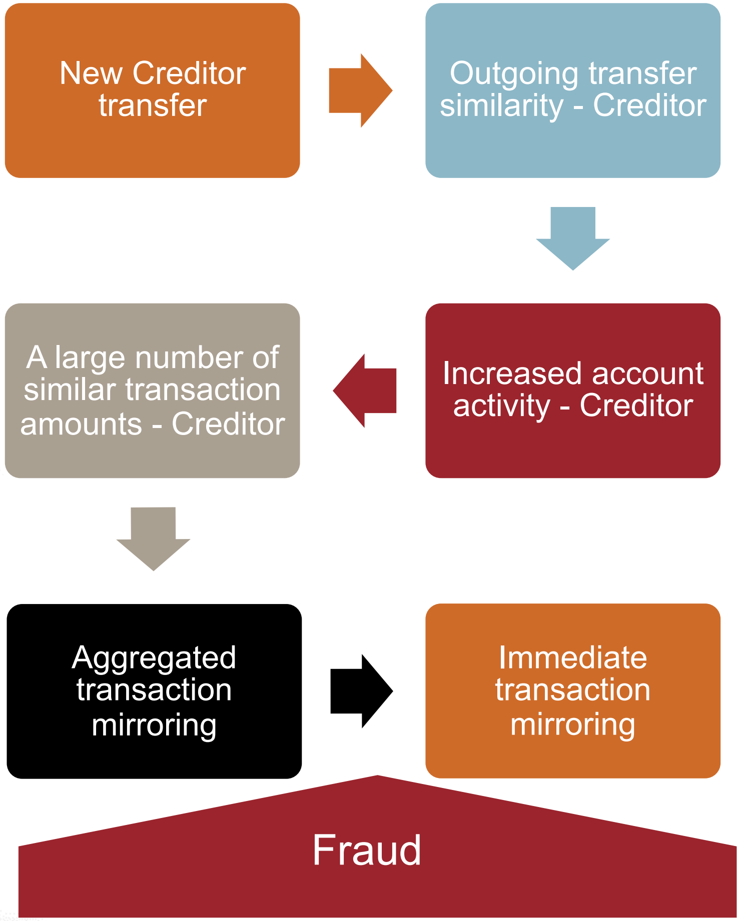
28. False promotions, phishing, or social engineering scams, such as fraudsters impersonating providers and advising customers that they have won a prize in a promotion and to send money to the fraudster's number to claim the prize.

DO THE ACTIONS SHOW A PATTERN OF FRAUD?

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.

Typology 28 (Scams)

003@1.1.0	Rule: Account dormancy - creditor
008@1.0.0	Rule: Outgoing transfer similarity - Creditor
010@1.0.0	Rule: Increased account activity - Debtor
011@1.0.0	Rule: Increased account activity - Creditor
016@1.0.0	Rule: Transaction convergence - creditor
018@1.0.0	Rule: Exceptionally large outgoing transfer
021@1.0.0	Rule: A large number of similar transaction amounts
025@1.0.0	Rule: Aggregated transaction mirroring
027@1.0.0	Rule: Immediate transaction mirroring
028@1.1.0	Rule: Debtor age
030@1.0.0	Rule: New Creditor transfer
034@1.0.0	Rule: Watch-listed account - Debtor
035@1.0.0	Rule: Watch-listed account - Creditor
036@1.0.0	Rule: Watch-listed party - debtor
037@1.0.0	Rule: Watch-listed party - creditor
048@1.0.0	Rule: Large transaction amount vs history - Debtor
063@1.0.0	Rule: Synthetic data check - Benford's Law - Creditor



New Creditor transfer

Outgoing transfer similarity - Creditor

Increased account activity - Creditor

A large number of similar transaction amounts - Creditor

Aggregated transaction mirroring

Immediate transaction mirroring

Fraud

A GROUP OF USER'S ACTIONS

Users act, rules are assessed, and you look for patterns of fraud, or typologies.

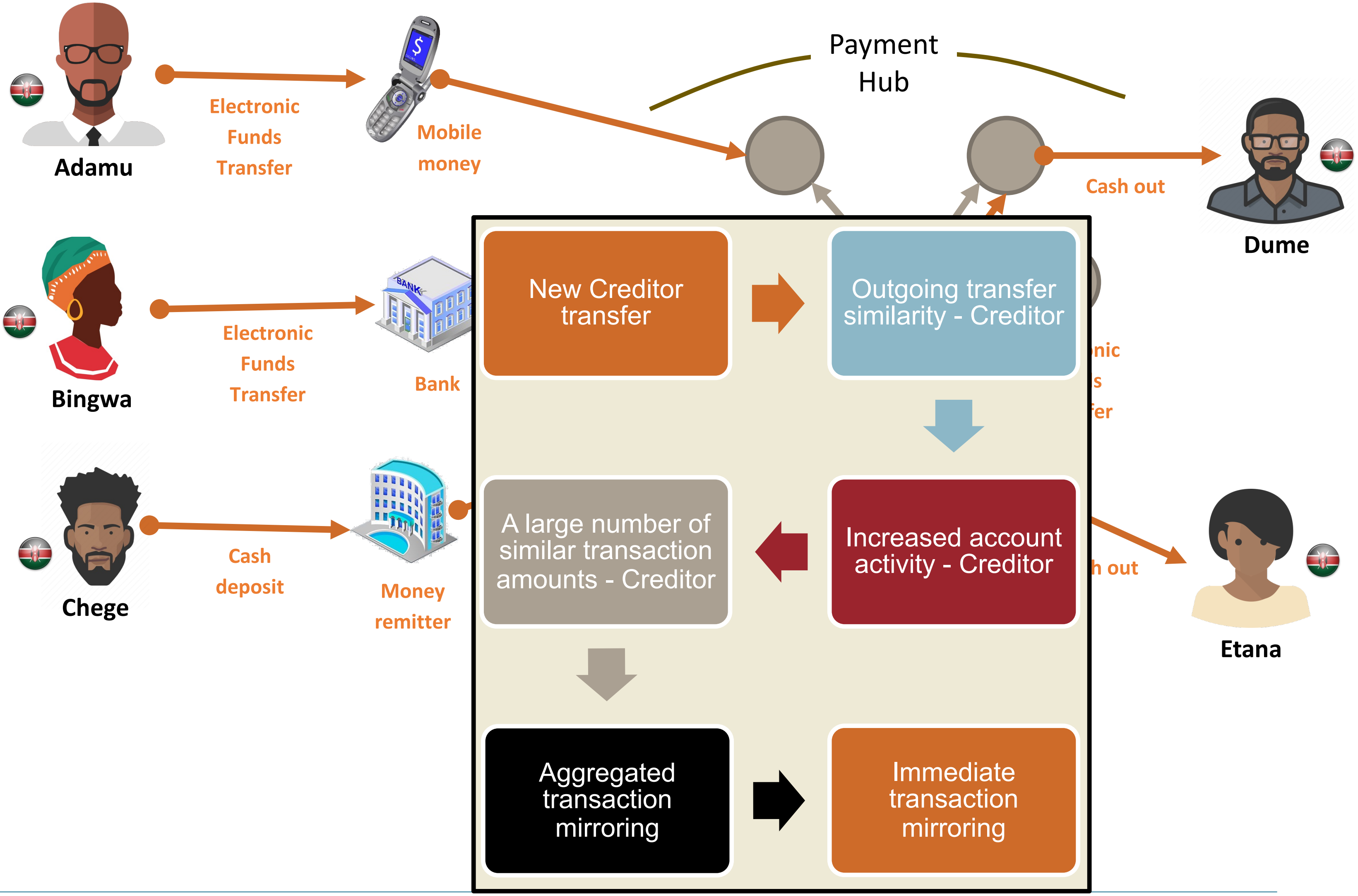
28. False promotions, phishing, or social engineering scams, such as fraudsters impersonating providers and advising customers that they have won a prize in a promotion and to send money to the fraudster’s number to claim the prize.

Adamu, Bingwa and Chege were convinced by Etana that they’d won a prize and needed to pay a small administration fee to Etana to process their winnings.

They each transfer the money to Etana’s account.

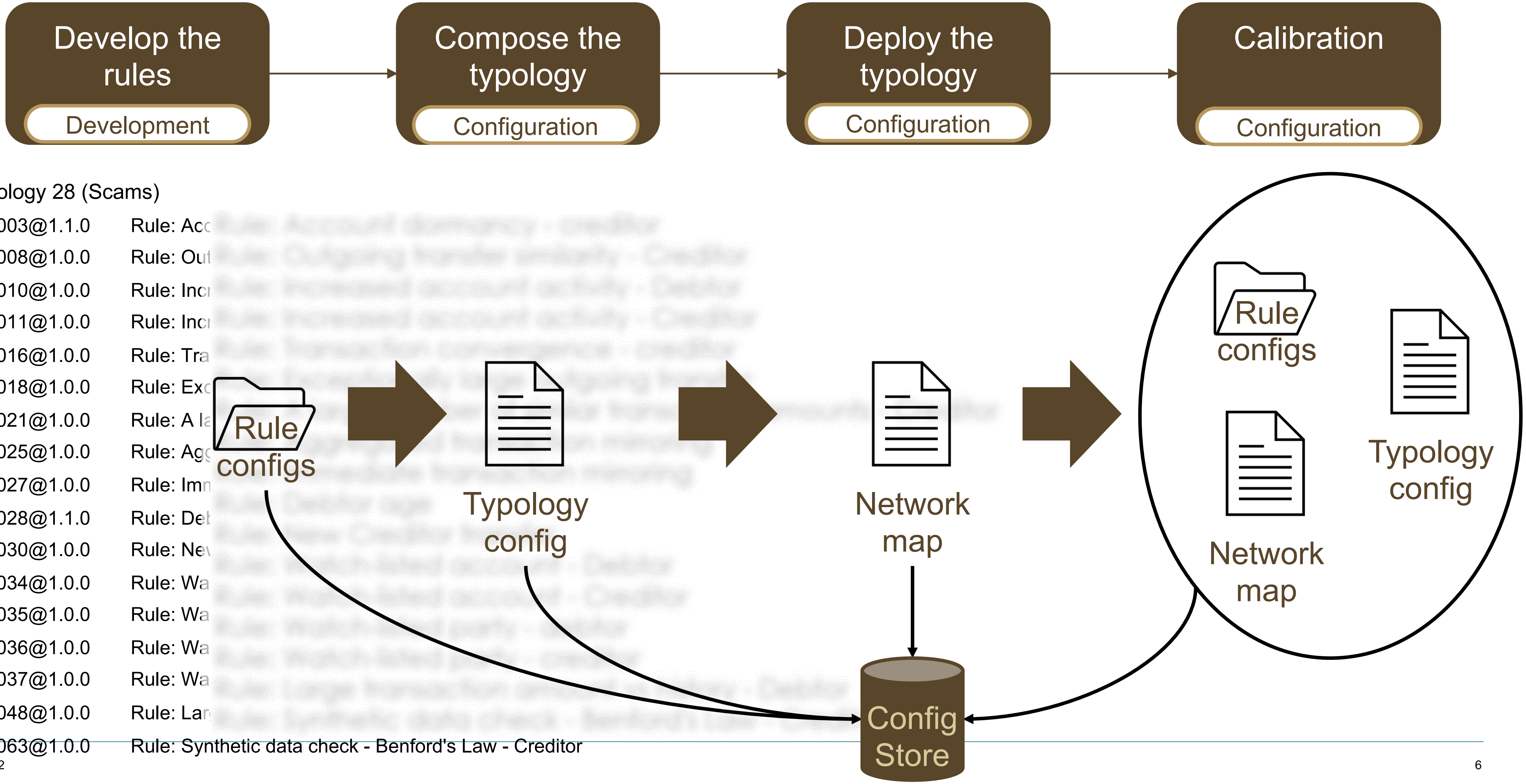
As each payment arrives, Etana immediately cashes out the payment. Adamu’s payment arrives after the money agent has closed for the day and Etana immediately transfer his payment to her associate, Dume.

Dume cashes out the payment first thing the next morning.



New Creditor transfer → Outgoing transfer similarity - Creditor → Increased account activity - Creditor → A large number of similar transaction amounts - Creditor → Aggregated transaction mirroring → Immediate transaction mirroring

THE TYPOLOGY LIFE-CYCLE

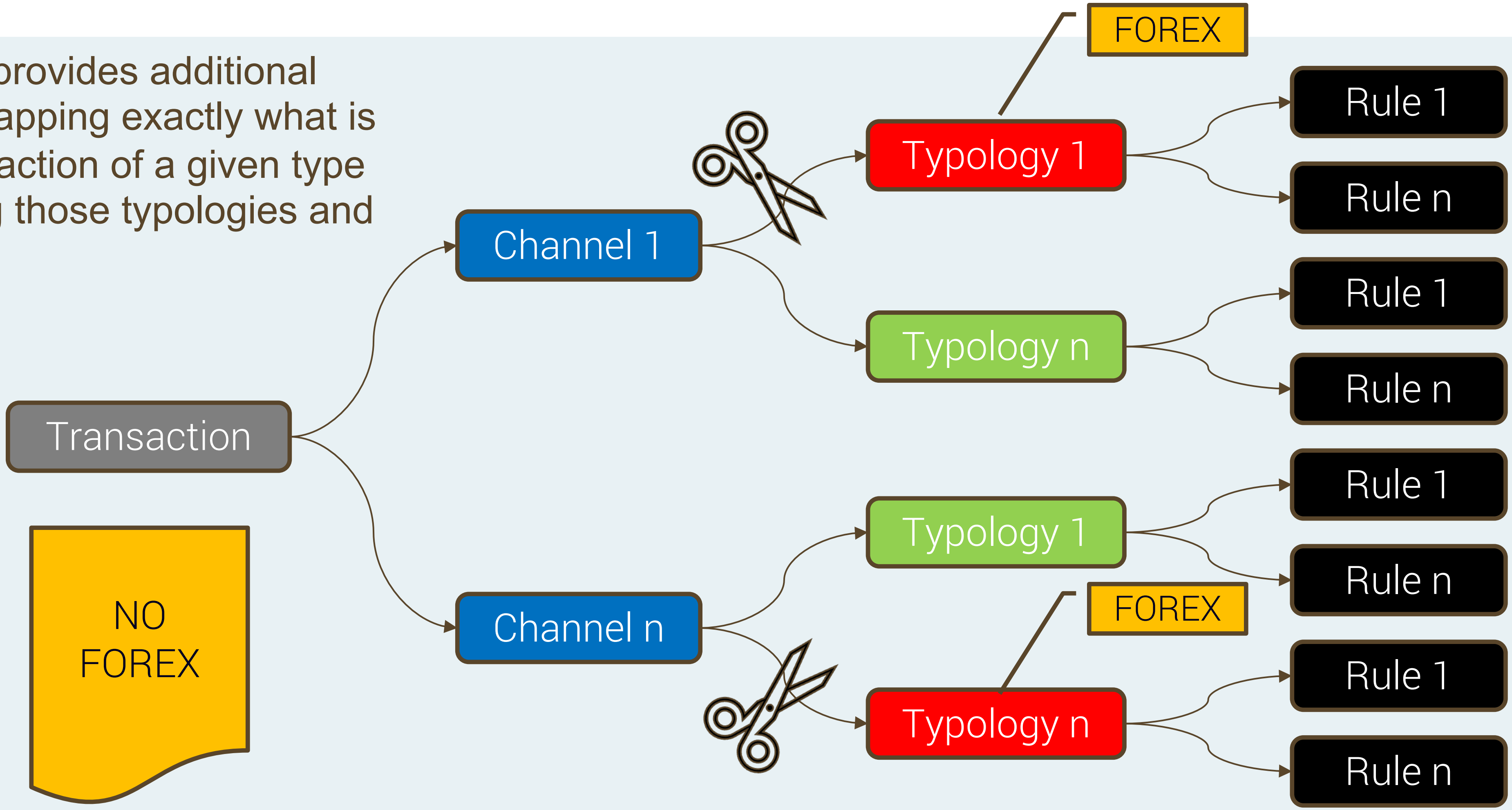


Typology 28 (Scams)

003@1.1.0	Rule: Acc
008@1.0.0	Rule: Out
010@1.0.0	Rule: Incr
011@1.0.0	Rule: Incr
016@1.0.0	Rule: Tra
018@1.0.0	Rule: Exc
021@1.0.0	Rule: A la
025@1.0.0	Rule: Agg
027@1.0.0	Rule: Imm
028@1.1.0	Rule: Deb
030@1.0.0	Rule: New
034@1.0.0	Rule: Wa
035@1.0.0	Rule: Wa
036@1.0.0	Rule: Wa
037@1.0.0	Rule: Wa
048@1.0.0	Rule: Lar
063@1.0.0	Rule: Synthetic data check - Benford's Law - Creditor

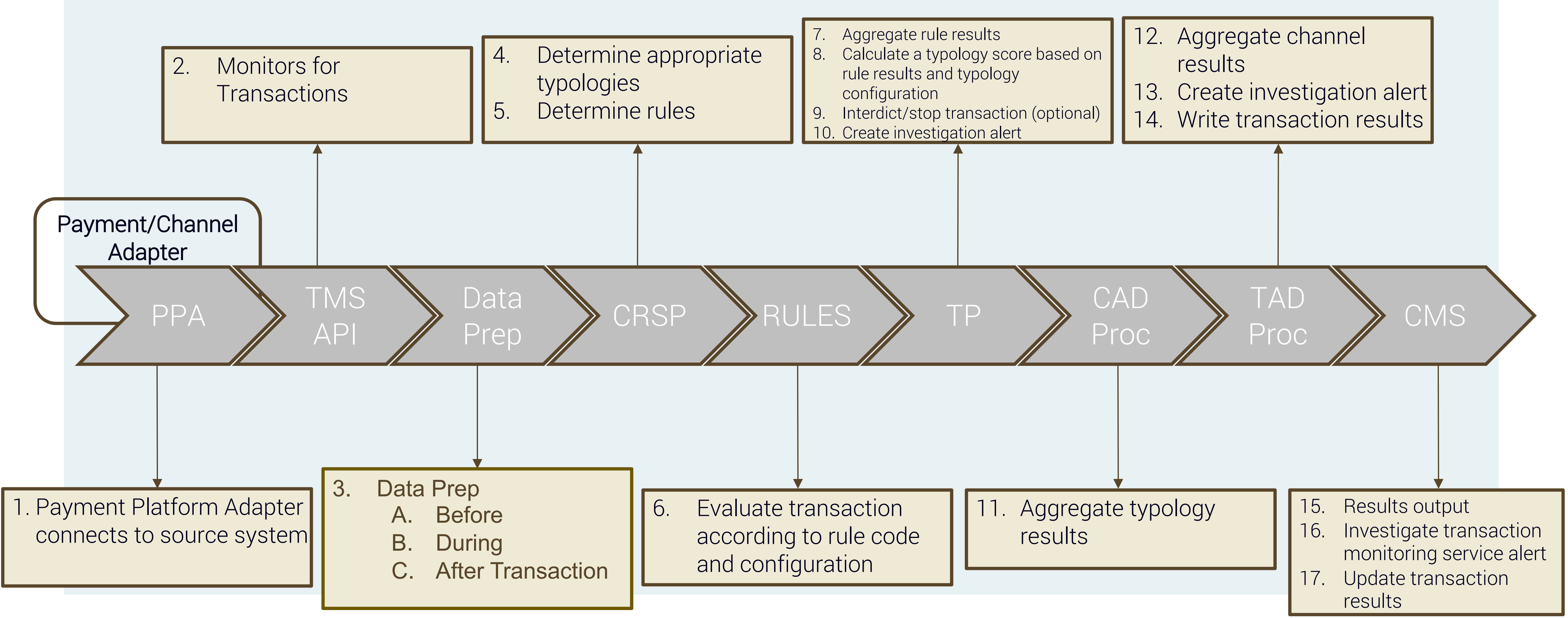
THE NETWORK MAP

The network map provides additional performance by mapping exactly what is needed for a transaction of a given type and only executing those typologies and rules.



PROCESS FLOW

As it is



1. Payment Platform Adapter connects to source system

2. Monitors for Transactions

3. Data Prep
   - A. Before
   - B. During
   - C. After Transaction

4. Determine appropriate typologies
5. Determine rules

6. Evaluate transaction according to rule code and configuration

7. Aggregate rule results
8. Calculate a typology score based on rule results and typology configuration
9. Interdict/stop transaction (optional)
10. Create investigation alert

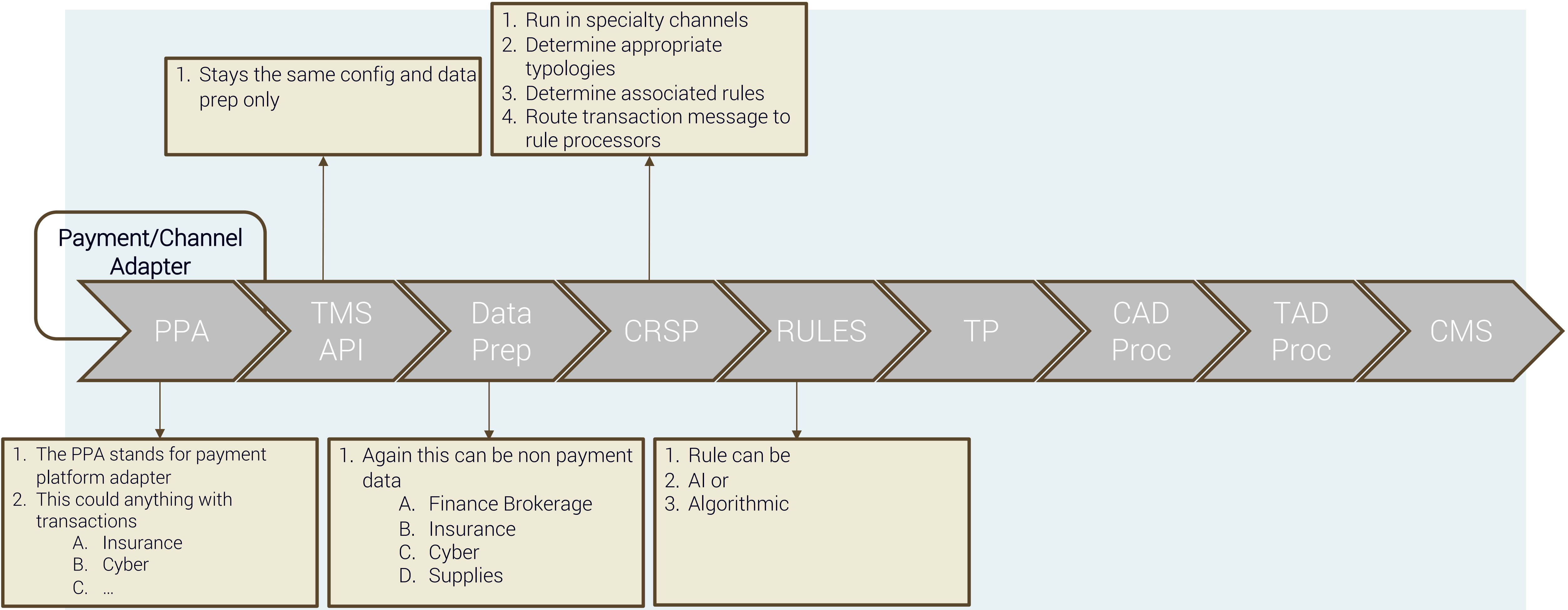
11. Aggregate typology results

12. Aggregate channel results
13. Create investigation alert
14. Write transaction results

15. Results output
16. Investigate transaction monitoring service alert
17. Update transaction results

PROCESS FLOW ADAPTIONS

Process flow options. What it can be …



Payment/Channel Adapter

PPA → TMS API → Data Prep → CRSP → RULES → TP → CAD Proc → TAD Proc → CMS

TMS API:

1. Stays the same config and data prep only

CRSP:

1. Run in specialty channels
2. Determine appropriate typologies
3. Determine associated rules
4. Route transaction message to rule processors

PPA:

1. The PPA stands for payment platform adapter
2. This could anything with transactions
    - A. Insurance
    - B. Cyber
    - C. …

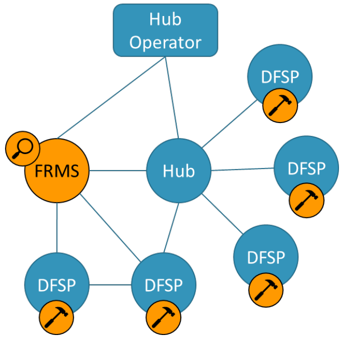
Data Prep:

1. Again this can be non payment data
    - A. Finance Brokerage
    - B. Insurance
    - C. Cyber
    - D. Supplies

RULES:

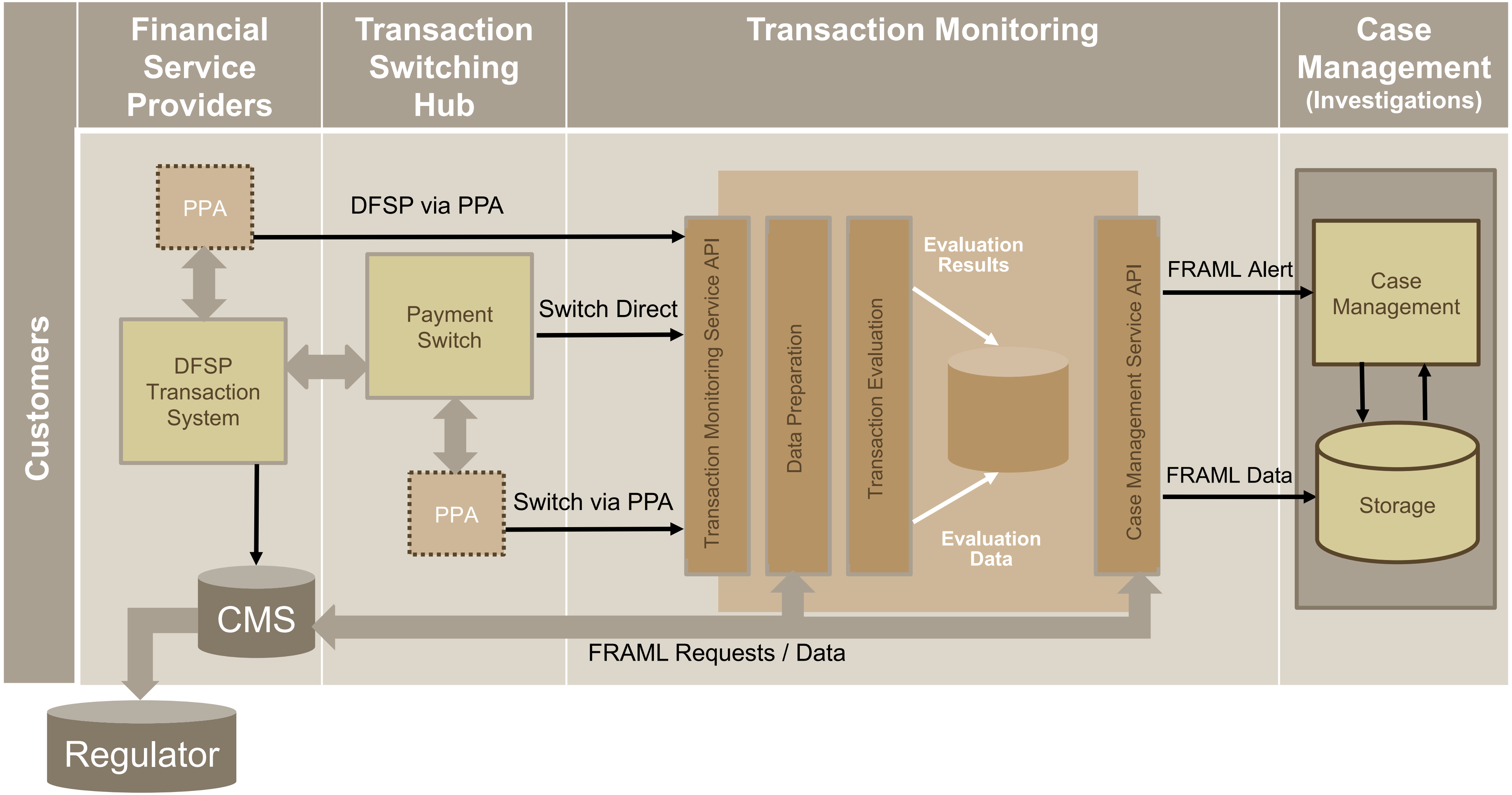
1. Rule can be
2. AI or
3. Algorithmic

OSS TMS CONTEXT



Semi-attached

- Centralised financial crime 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 DFSP would employ compliance teams



WHY AN OPEN-SOURCE FRAUD RISK MANAGEMENT SYSTEM?

“With more than 4.5 billion people online, more than half of humanity is at risk of falling victim to cybercrime at any time, requiring a unified and strong response.”

Jürgen Stock, INTERPOL Secretary General

Open Source = Lower Costs

- **Fraud is a major issue—and it’s getting worse**
- **Fraud is expensive**
  - **to those who are defrauded**
  - **to the system – defending against fraud costs tremendous amount to each player in the ecosystem**
  - **to government, both dealing with their own fraud, and helping others to defend against it.**

- **Human impact**
- **Government outcomes impact**
- **Reputational impact**
- **Government systems impact**
- **Industry impact**

- **Environmental impact**
- **Security impact**
- **Financial impact**
- **Business impact**

Based on international estimates, public bodies generally lose between 0.5% and 5% of their spending to fraud and related loss.

The private sector fears reputational impact and does not generally disclose, but according to Merchant Savvy, global losses of payment fraud have tripled to $32.39 billion in 2020 and are expected to continue to cost $40.62 billion in 2027 which is 25% higher than in 2020.

Therefore, the increase in fraud cases restrains the growth of the payments markets and financial inclusion, and this largely ignores informal markets.

International Public Sector Fraud Forum Guide to Understanding the Total Impact of Fraud February 2929

OPEN-SOURCE TRANSACTIONAL MONITORING SYSTEM

- **We started with an Open-Source TMS because it's**
  - Typically, the most complex component of an overall Fraud Risk Management System (FRMS)
  - Typically, the hardest component of an overall Fraud Risk Management System (FRMS) to implement
  - Typically, the most expensive component of an overall Fraud Risk Management System (FRMS)
  - Typically, it has the most room for improvement
- **Goal - Making one system that both scales up and down, is performant and solves more than one problem (payments, cyber, internal fraud).**
- **We have succeeded, but of course there is more to be done.**

Why?

"We choose to ~~go to the moon~~ *Build a TMS* in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one which we intend to win."

— John F. Kennedy

It produces the biggest impact.

Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Open_source

• UNIQUE FEATURES

- **An engine only.**
  - Designed to be used by anyone and modified for their own needs or as the plumbing of a solution offered by a commercial entity.
  - API driven
  - Highly configurable by Json message
  - Modular and adapter driven both for data/events in and data/events out to the line of business systems and case management system
- **Scales up and Down to run in the smallest and most limited of situations as well as country-wide payment switches, banks, or payment networks**
- **We Pseudonymize Data**
  - Why pseudonymize? - to fulfill data protection by design
    - All platform activities are logged in detail, but logs should not expose PII data
    - Pseudonymization of personal data provides an additional layer of protection in the face of a data breach
    - Protection and obfuscation of PII data during investigations – limits visibility to a “need to know”

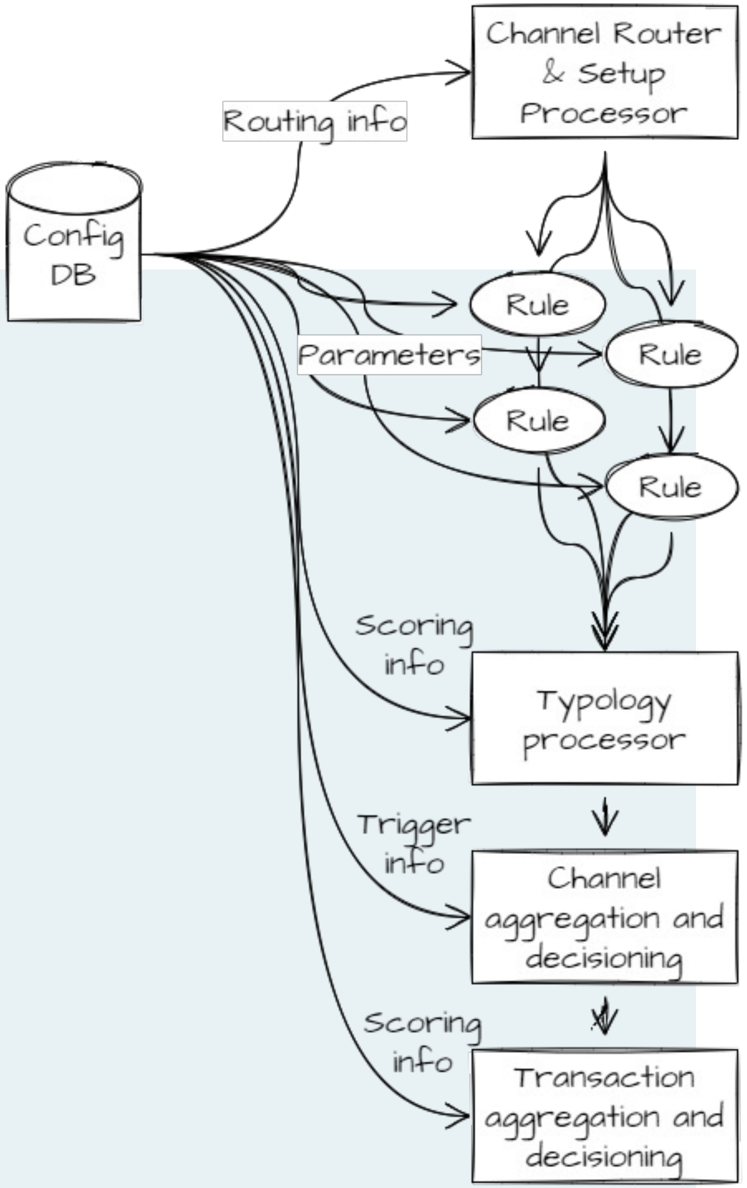
• UNIQUE FEATURES (CONT’D - 2)

- **The unique channel-driven design allows for the creation of channels for processing interdictive, immediate, near-time, batch typologies.**
  - Each channel can be tuned uniquely for performance and the consumption of resources.
  - A network map per payment or other transaction to be analyzed:
    - Determines the types of typologies to be run for the transaction type
    - Determines the rules to be run for the typologies and is run exactly once
      - Very efficient use of system resources and provides a massive performance boost

UNIQUE FEATURES (CONT'D - 3)

Configuration-Driven Design

- Soft-coding vs hard-coding
- We abstracted the configuration of processors:
  - Channel Routing and Setup Processor
    - Routing via a network map that is dynamically composed based on transaction attributes
  - Rules Processors
    - Channel and typology routing information via a network map
    - Rule parameters
  - Typology Processor
    - Channel and rule routing information via a network map
    - Typology expression
    - Typology scoring
  - Channel Aggregation and Decisioning Processor
    - Typology routing information via a network map
    - Typology trigger information
  - Transaction Aggregation and Decisioning Processor
    - Channel routing information via a network map
    - Transaction scoring



Channel Router & Setup Processor
Routing info
Config DB
Rule
Parameters
Rule
Rule
Rule
Scoring info
Typology processor
Trigger info
Channel aggregation and decisioning
Scoring info
Transaction aggregation and decisioning

xxx

FRAUD RISK MANAGEMENT SYSTEMS CENTER OF EXCELLENCE

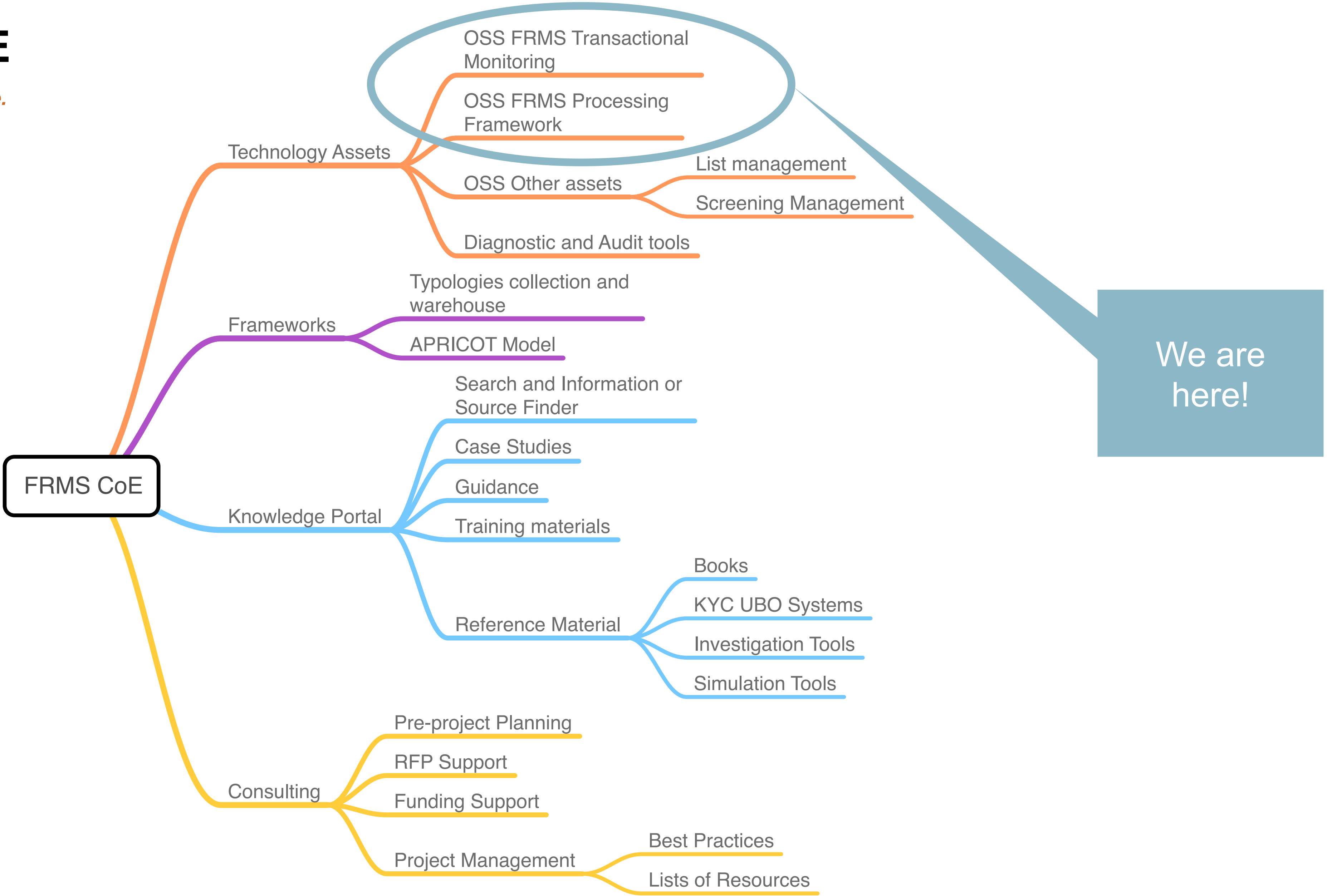
FRMS CoE

- The FRMS CoE is barely a thing
  - Being shaped and built as we speak – complete EOY
  - Main & First job is to manage the OSS TMS the FRMS MVP created
- Access is coming
  - https://github.com/frmscoe - GitHub
  - https://frmscoe.atlassian.net/ - Documentation & Jira
  - johannes@frms.io - Johannes Foley will get you access
    - Let’s use this email and not clog his work address
  - All will be available by the end of August – including CI/CD instructions
  - Typologies will be managed separately

Let’s Move Forward

FRMS COE

What it might look like.



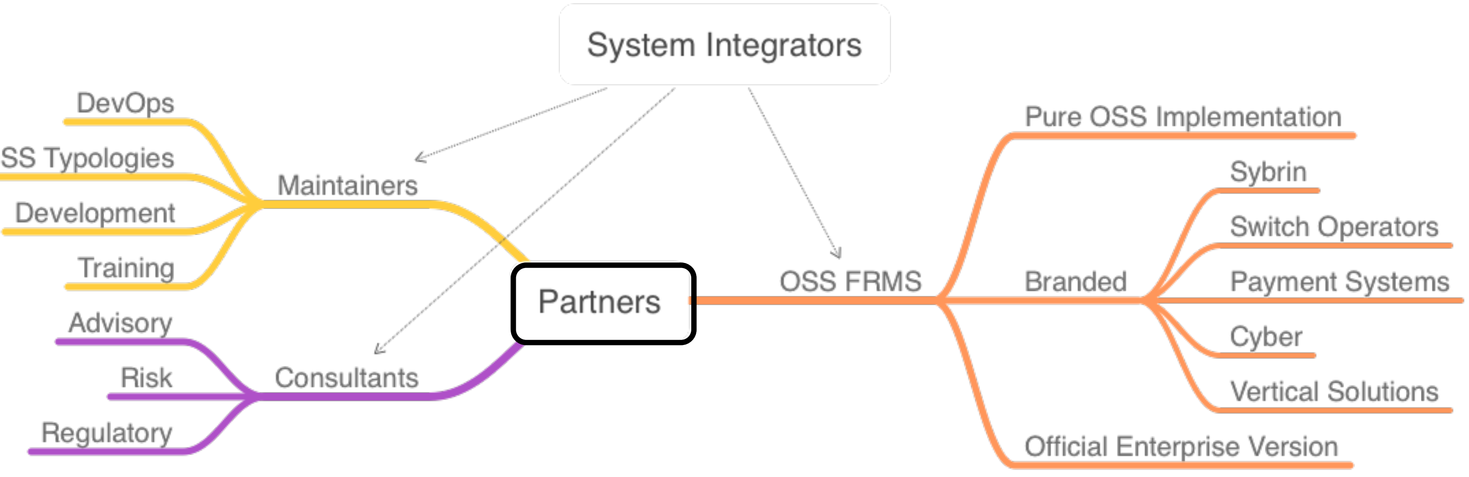
WE NEED HELP

We are at the beginning …

Contact

Greg McCormick, greg@frms.io

Johannes Foley, johannes@frms.io



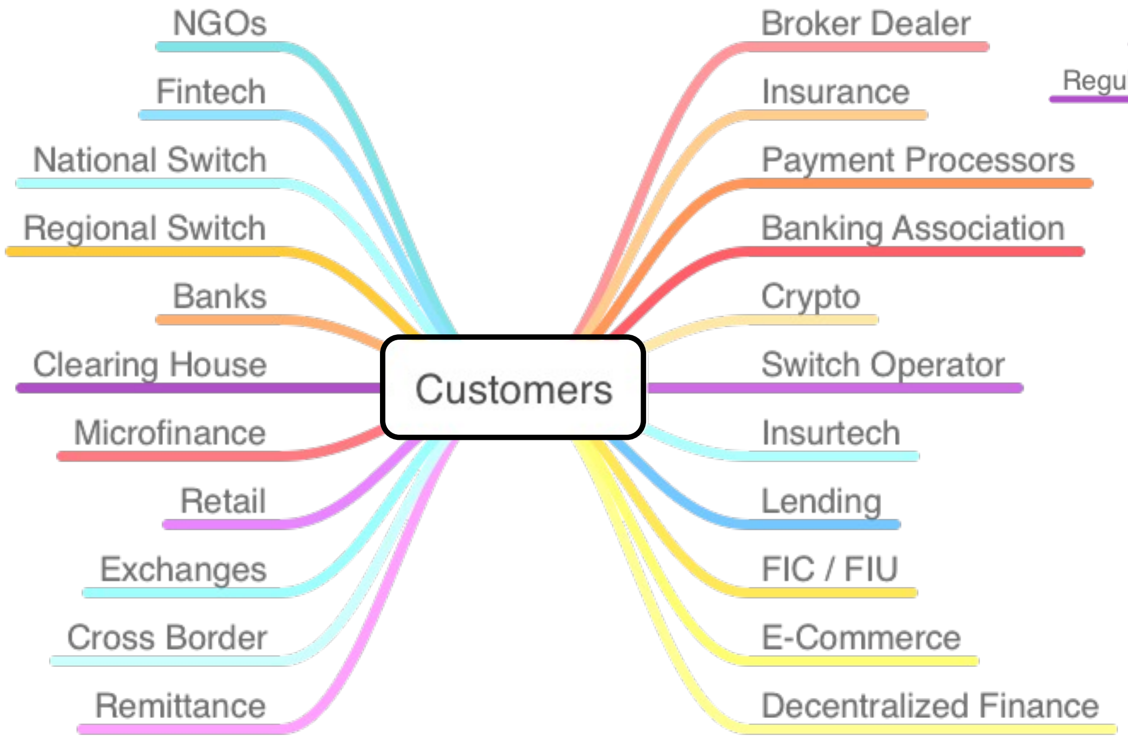
System Integrators

Partners

Maintainers: DevOps, OSS Typologies, Development, Training

Consultants: Advisory, Risk, Regulatory

OSS FRMS: Pure OSS Implementation; Branded (Sybrin, Switch Operators, Payment Systems, Cyber, Vertical Solutions); Official Enterprise Version



Customers

NGOs, Fintech, National Switch, Regional Switch, Banks, Clearing House, Microfinance, Retail, Exchanges, Cross Border, Remittance

Broker Dealer, Insurance, Payment Processors, Banking Association, Crypto, Switch Operator, Insurtech, Lending, FIC / FIU, E-Commerce, Decentralized Finance

- Subject Matter Experts
- Advisory Consultants
- Customers to test
- System Integrators
- Customers for engagements
- OEMs

CONTACTS

- Roland Van Hee – CTO, Technical Governing Board, email: Roland.VanHee@sybrin.com
- Jason Damanovich - CIO and BU head for Open-Source Initiative including Mojaloop, email: Jason.Darmanovich@sybrin.com
- Johannes Foley – DA Member and Product Manager, Mojaloop and Fraud Risk Management, email: Johannes.Foley@sybrin.com
- Salvatore Errera - Product Manager Onboarding and Biometrics, Business Interface for “Actio” FRMS TMS, email: Salvatore.Errera@sybrin.com

- The Fraud Risk Management Systems Center of Excellence (FRMS CoE)
  - Web Site, don’t expect much yet, www.frms.io
  - Greg McCormick, Executive Director of the FRMS CoE, email: greg@frms.io