wibmo
a PayU company

Seamless security @ Scale

WIBMO PROTECT

CONTEXTUAL AUTHENTICATION

JUNE 2023

Global Payment Fraud Losses

41
BILLION USD
2022

48
BILLION USD
2023
(expected)

Source : www.statista.com

Emerging Fraud in addition to the traditional Modus Operandi

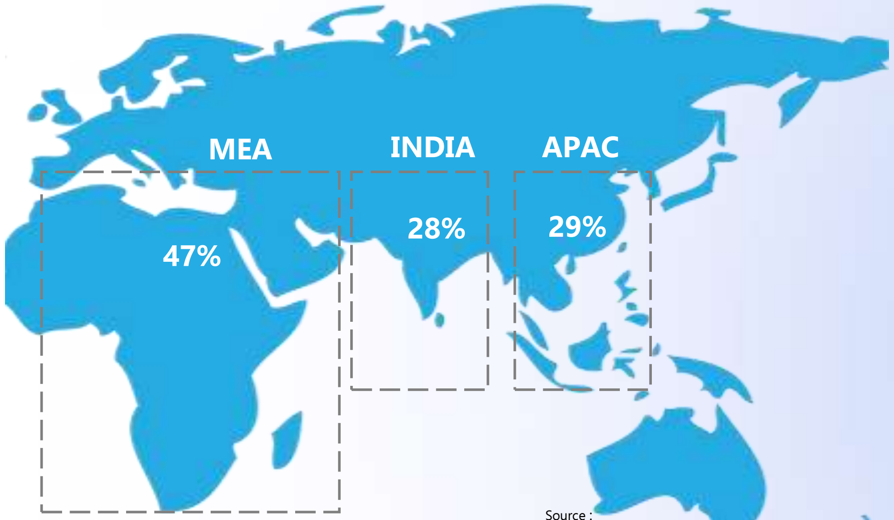
- **Silent Frauds**: small amounts are taken from thousands of accounts – the whole adding up to often more than a single large fraud event
- **Triangulation** : fraudster posts a product online at a severely discounted price, which is purchased by a customer using a valid credit card
- **Pagejacking** : copying of a legitimate website and using it to spoof customers to take payments
- **CXO Frauds** : fake instructions from someone posing as a manager typically asking you to make a payment or transfer money.

Cost of fraud goes beyond the lost transaction value itself

TRUE COST OF FRAUD

- Lost goods or merchandise
- Manual Review
- Chargeback Fees
- Low Success Rate – Order declined due to stringent rules
- Cost of in-house fraud prevention system
- Cost of shipping
- Processing fee for the transaction
- Cost of employee – customer support, investigations and audits

Card Based eCom Sales



Source :
https://www.ppro.com/regions/middle-east-africa/
https://www.ppro.com/countries/india/
https://www.ppro.com/regions/asia-pacific/

3D Secure Geographical Nuances

- According to Boston Consulting Group, $5 trillion in annual global retail sales shifted from offline to online due to the pandemic
- The overall percent of global transactions identified as potential fraud ranged between 10 to 13%
- $16 billion is the cost of fraud and theft for consumers in 2020.(JP Morgan report)

INDIA

- 2FA is mandated by RBI to increase the security of all digital transactions,SMS based OTP has become a go to mechanism.
- RBI is set to explore alternate risk-based authentication mechanisms leveraging behavioural biometrics, location / historical payments, digital tokens, in-app notifications, etc
- Mastercard, Visa , American Express have extended support for 3DS 1.0 support till October 2023

MEA

- in this region, 3DS1.0 transactions will not be supported by the directory servers.
- Banks have less restriction to explore other modes of authentication such as Biometric
- Mastercard came into partnership with Network International, the leading enabler of digital commerce in the Middle East and Africa (MEA).

APAC

- The Asia-Pacific region is projected to undergo substantial during the forecast period due to the increasing growth of IT technology.
- Visa extended 3DS 1.0 support Bangladesh, Bhutan, Maldives, Nepal, and Sri Lanka through October 12, 2023.

Payment Security & Compliance

Problem Statement

RISK CONTAINMENT

Fraud Risk

- Monitoring
  - Financial Transactions
  - Non-Financial Transactions
- Prevent Fraud & Abuse

Compliance Risk

- 3DS 2.0, PSD2, BSP 1140
- Reporting

CONVENIENCE & SPEED

Customers

- Seamless user experience
  - Authentication Methods
  - Quick Checkouts
- High Security & Assurance

Banks

- Seamless Investigation Flow
  - Holistic Risk View
  - Quick Alert Disposition

TECHNOLOGY

Scalable, Secure And Reliable

- < 100 ms ; 1200 TPS; 99.9% availability
- On Cloud/ On Premise

COST OF OPERATIONS

Lower TCO

- Reduced Business Decline
- Lower Administrative Cost

Wibmo Protect Overview

End to End Solution

Comprehensive End to End solution that does compliance, risk and multi-factor authentication

Scheme Agnostic

Use intelligence derived from transactions across Visa, MC, AMEX, DINERS, JCB, CUP

Knowledge Base

Out of box 100+ scenarios for risk containment pertaining to various payment methods

WIBMO PROTECT CONTEXTUAL AUTHENTICATION

Secure, Seamless, Scalable

Fraud Prediction

Predicts Cardholder Fraud leveraging Rules and customizable AI/ML Models

Data Enrichment

Ability to connect to external systems and flexibility to fetch data and expose APIs

Fast Onboarding

Ready to service transactions in less than 6 weeks on a Scalable, High Available, Cloud ready platform

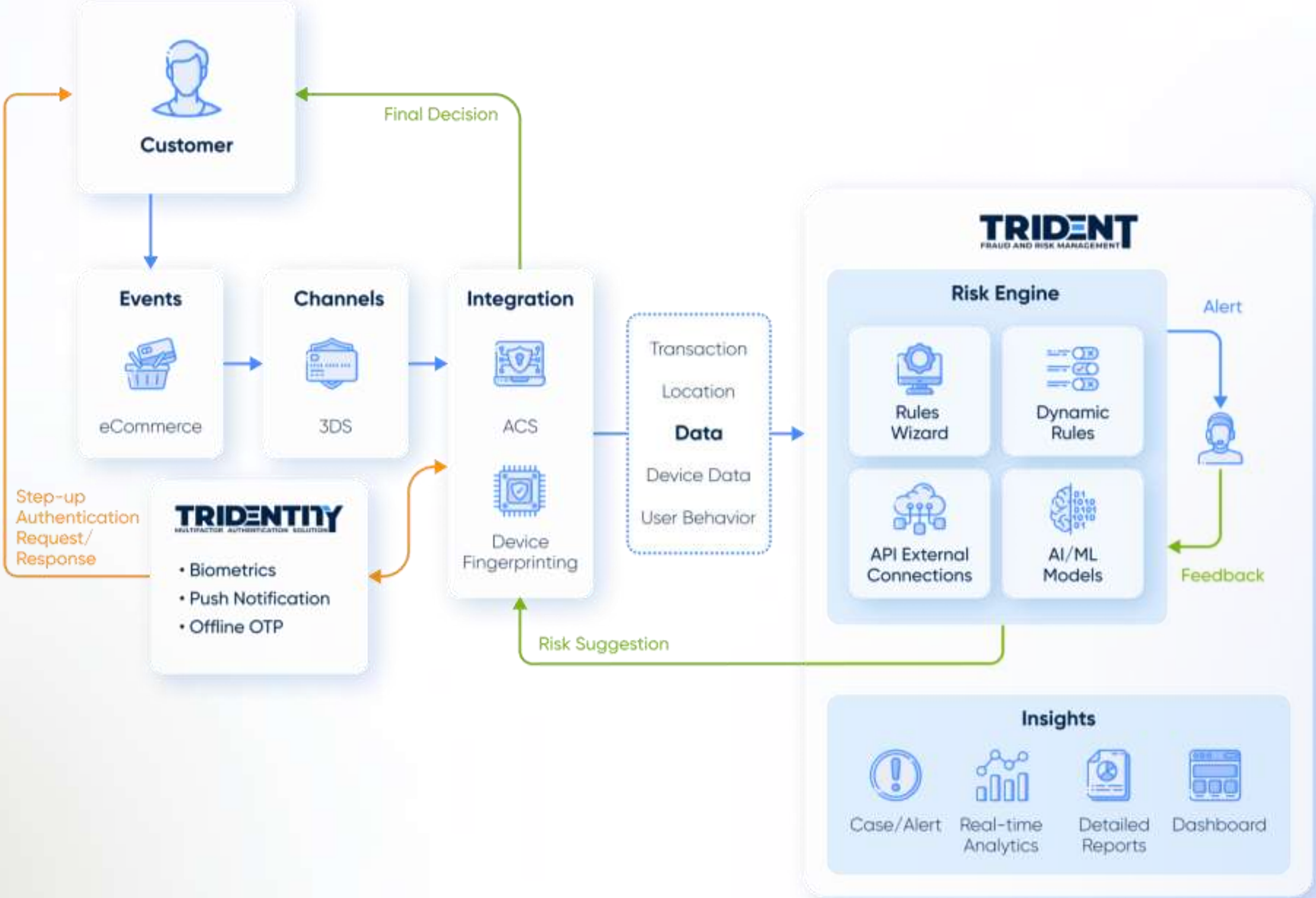
IMPROVE
Risk Containment

IMPROVE
Operational Efficiency

REDUCE
Customer Friction

QUICK & EASY
Deployment

Solution Journey The Big Picture



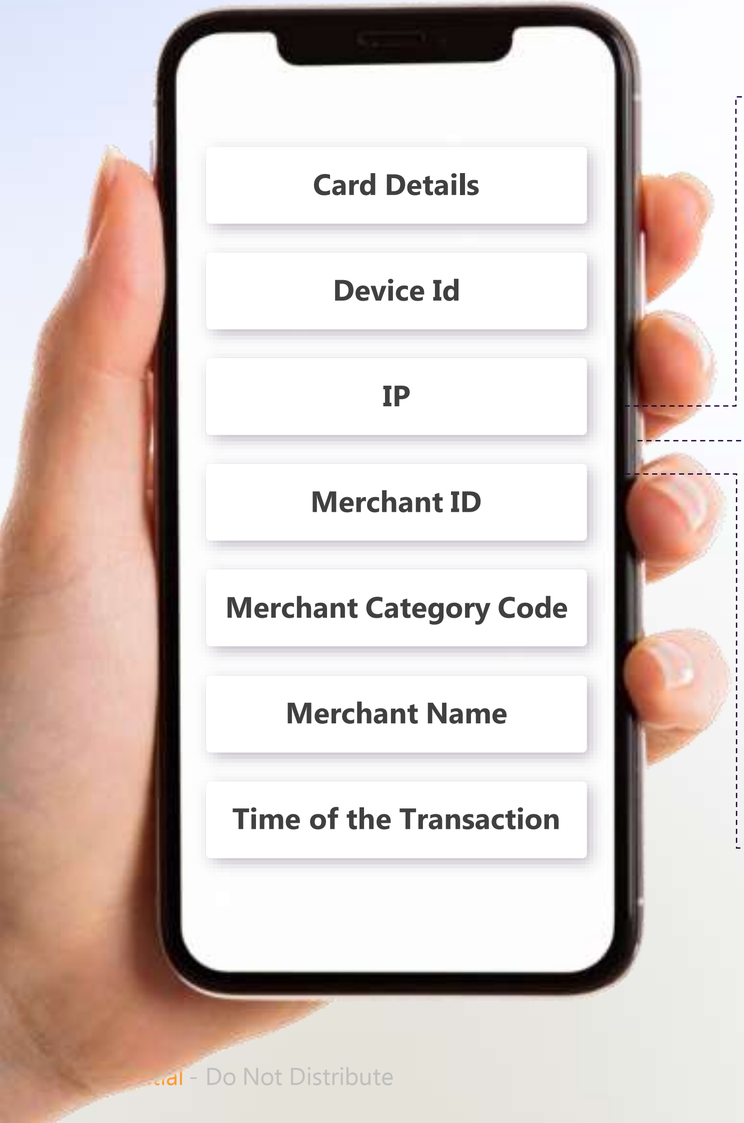
Use Cases

	Transaction				Device					
	Merchant ID	IP	Transaction Time	Amount	Jailbroken Rooted	Screen Mirror	Malware Installed	On Call	RISK SCORE	
UC 1 Step Up Authentication	Usual Merchant	Unusual IP Address	Business Hours	Unusual Amount	NO	YES	NO	YES	MEDIUM	CHALLENGE
UC 2 Decline Transaction	Usual Merchant	Unusual IP Address	Business Hours	Usual Amount	YES	YES	YES	YES	HIGH	DECLINE

Additional Use Cases

- Creation and utilisation of Blacklist
- Last 30 day purchase > 2 Lakhs
- UPI Onboarding : Bank A/C linking threshold
- Electricity bill payments > 1 Lakhs

Wibmo Protect Scenarios



- Card Details
- Device Id
- IP
- Merchant ID
- Merchant Category Code
- Merchant Name
- Time of the Transaction

Velocity

SAME BIN TRANSACTIONS

- Multiple transaction attempts from same BIN cards in short period of time

TRANSACTION BURST

- Multiple transactions initiated from same IP/Device in short period of time

Phishing

UNUSUAL BEHAVIOUR

- High value transaction towards a new merchant
- Transaction value higher than the transactions done in last 6 months

FIRST TIME

- Transaction from a new device, IP and location
- Transaction towards a new merchant or in foreign currency

Negative List

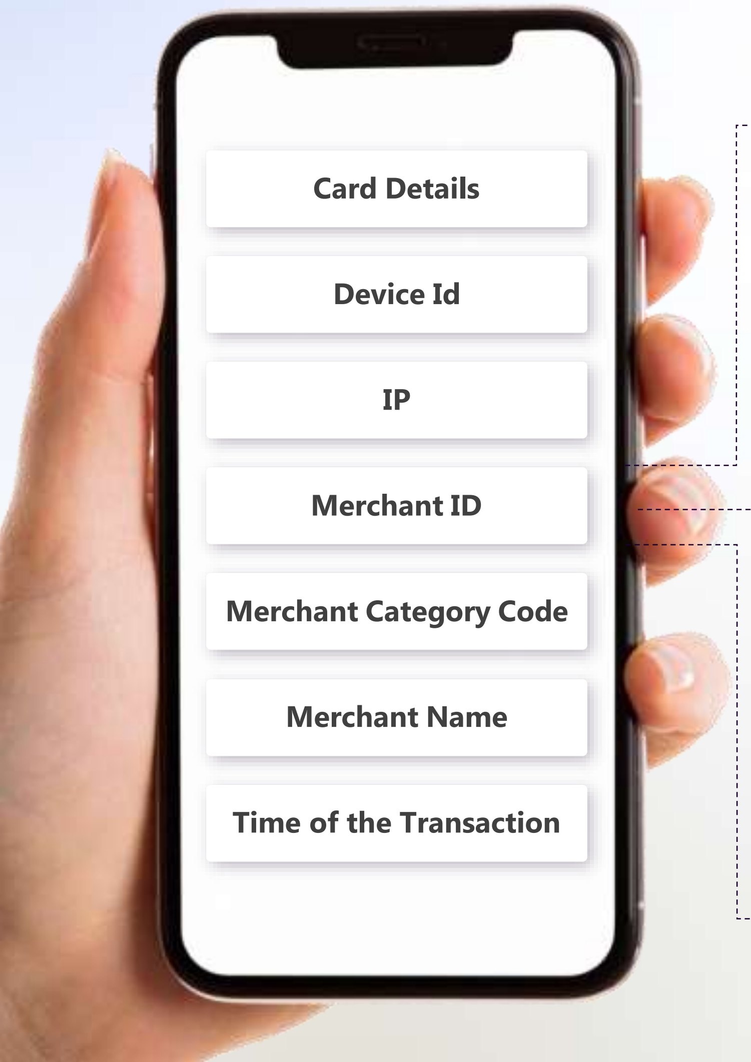
SUSPICIOUS GEOGRAPHY

- Transactions initiated towards payee with IP from blacklisted geography

SUSPICIOUS TIME PERIODS

- Count of failed high value transactions initiated during odd hours (eg: 12:01am – 5 am) is greater than the defined threshold

Wibmo Protect Scenarios



- Card Details
- Device Id
- IP
- Merchant ID
- Merchant Category Code
- Merchant Name
- Time of the Transaction

Merchant

SUSPICIOUS MERCHANTS

- Transaction towards High Risk Merchants or merchants belonging to Suspicious Merchant Category Codes.

HIGH VELOCITY

- Multiple failed transactions towards same Merchant from same BIN/IP/DEVICE

Source

SEEKING DONATION/SUPPORT IN THE NAME OF FAKE BENEFICIARIES

- P2P transactions towards the beneficiary / VPA containing suspicious keywords like (Refund, Support, Army, Relief, Claim, Minister, reward, cashback)

MALICIOUS GOOGLE ADS

- Burst of transactions initiated from same Google Ad ID (link)

User Behavior

USUAL BEHAVIOUR

- Transactions initiated from a device which has been used for successful transactions on unique days
- Transactions initiated from an IP which has been used for successful transactions on unique days
- Successful Transactions towards a merchant done on unique days

IVS - Introduction

Industry best solution in card-not-present and digital payment authentication built on the EMVco 3D secure protocol .

Provides perfect user experience across device channels with top notch security

IVS- Core Features

Certified for the latest EMVco protocol version 2.3.1

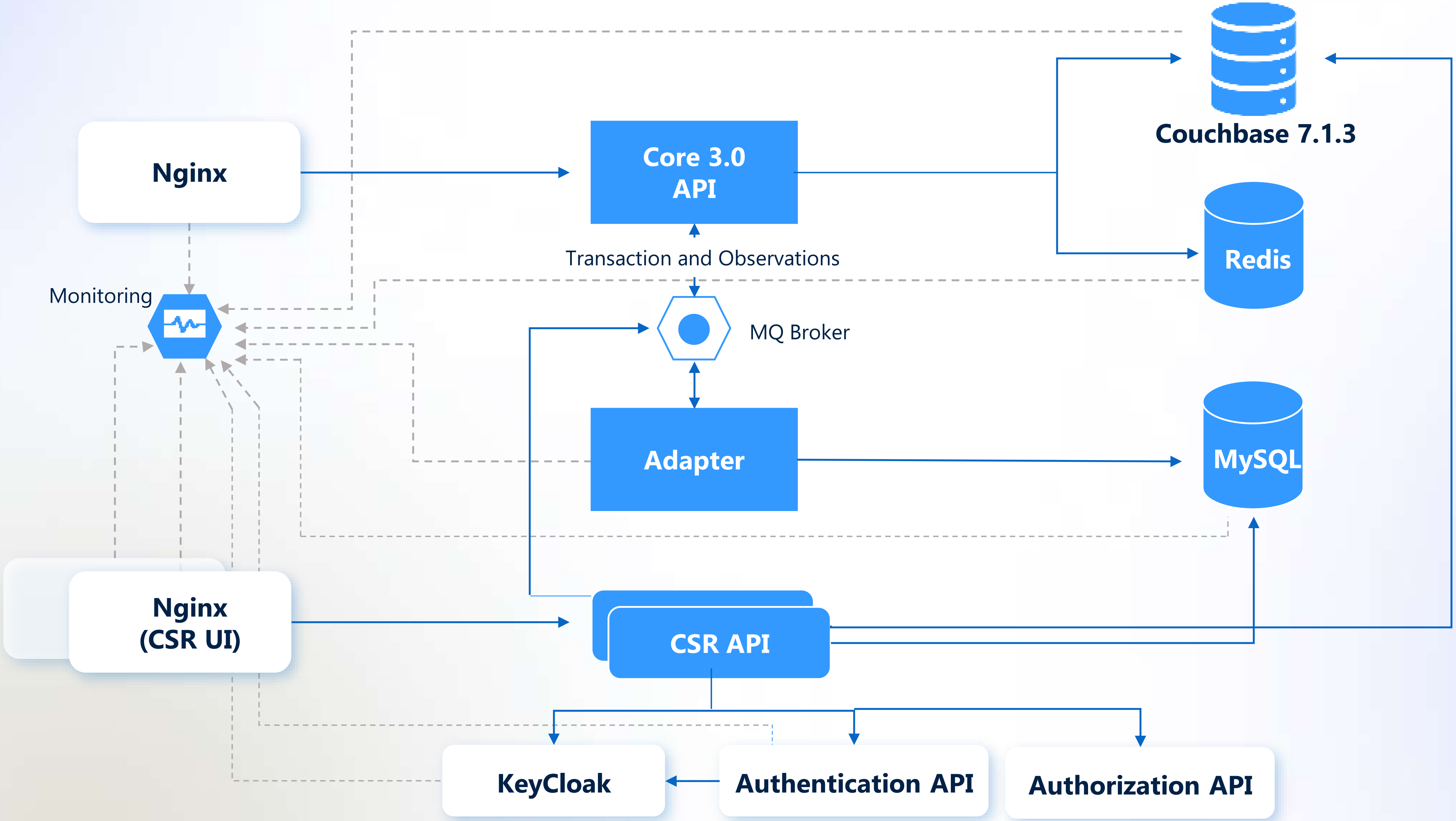
Supports all major card schemes (Visa, Mastercard, Diners, Amex, UPI, JCB)

Provides standalone static rule Engine, which can be used for first level of defense and support specific business requirements within the protocol definition

Supports customized ExpressPay solution to increase authentication rates and customer experience

True High availability and Dynamic load sharing using Continuous Available Architecture (CAA)

Technology Deployment



Trident RBA - Introduction

RBA determines transaction risk score, based on tolerance levels, and suggests the appropriate authentication method

Leverages risk-based authentication to award loyal users accessing websites and mobile apps.

Intelligent authentication combats fraud and offers seamless user experience

Why RBA

? Friction during payments leads to abandoned transactions
- Redirection leading to drops
- Consumers demands convenience & speed

Benefits

- Improved Success Rate (~2% - 6%)
- Increased Consumer Loyalty
- Increased Gross Merchandise Value (GMV)
- Reduced operational cost (SMS etc.) and cart abandonment
- Reduced False Positives

Finding the right balance between preventing fraud, reducing customer friction

Trident RBA - Features

Real-Time Risk Assessment

Process Automation

Reporting

Risk based Assessment & Monitoring

1

Transaction Monitoring

Monitor transactions against data points ranging across user profiles, purchase patterns, sessions, device and transactions details

2

Process Automation

Improve operational efficiency through multi-queuing functionality , user specific task assignment

3

Overall Risk Assessment

Augment profiling with continuously and quickly deployable rule engine to shield business

4

Reporting

Automated reporting based on the business needs to augment quick decision making

5

Real-Time Risk Control

Real time addition of riskier elements such as merchants, mcc, BINs etc for subsequent transaction protection

Trident RBA – Core Features

Certified for the latest EMVco protocol version 2.3.1

Supports all major card schemes (Visa, Mastercard, Diners, Amex, UPI, JCB)

Provides standalone static rule Engine, which can be used for first level of defense and support specific business requirements within the protocol definition

Supports customized ExpressPay solution to increase authentication rates and customer experience

True High availability and Dynamic load sharing using Continuous Available Architecture (CAA)

VCAS

Corporate Overview

Key Statistics

- Headquarters: Cleveland, OH
- Size: 11K employees

Key Dates

- 1999 – Cardinal Commerce founded
- 2015 – Nilson Report says VisaNet processes 100B txns in 2014
- In 2017, Visa acquired CardinalCommerce. This acquisition allows Visa to broaden their payment scope, giving Visa access to both issuer data and merchant data. This theoretically allows Visa to better detect fraud events due to the increase in size of the data they are collecting.

Product Offerings

- Visa Consumer Authentication for Issuers (VCAS)
  - VisaNet – The technology behind Visa. This is their vast network of electronic payment data that powers their models

Approach

For Issuers & Processors, VCAS drives multiple layers of protection against e-commerce fraud. Visa pushes the use of risk-based authentication and authorization solutions. VCAS includes:

- Sophisticated risk-based authentication
- Support for mobile
- Tailored rules for risk-decisioning capability
- Dynamic & Strong Authentication

Visa's transaction intelligence network now possesses Visa, merchant and issuer data with support for 3DS 1.x/2.0 and PSD2.

Commentary

VCAS has become the issuer solution going forward

Before the acquisition by Visa, CardinalCommerce provided issuers with its own 2IDentiFI solution. With the acquisition, the 2IDentiFI brand has been retired, and the best functionality from 2IDentiFI and Visa Consumer Authentication Service were merged into the new Visa Consumer Authentication Service solution. Customers of the legacy VCAS solution have been migrated to the new VCAS solution

Fraud Risk decisioning

CardinalCommerce uses a collaborative approach to risk decision-making. Cardinal Consumer Authentication facilitates the comparison (in real-time) of what banks know about their customers and what merchants understand about their consumers, tuning the combined results to optimize the consumer experience. Traditionally, solutions rely on two mutually exclusive parties to eliminate fraud, where merchants use fraud screening services and issuers use their version of risk mitigation technologies. Each of the parties attempt to assess which orders are "suspicious" and depending on their respective criteria, eliminate those orders. Merchants won't submit their suspicious orders for authorization and issuers will not authorize orders that fall under their specific criteria. Since these traditional systems are mutually exclusive, this grinds potential orders to the lowest common denominator of good orders. Cardinal Consumer Authentication creates a collaborative approach where there is visibility in how each side treats a transaction, helping increase the authorization yield. This can be thought of as a 2x2 decision matrix (i.e., yes/yes, yes/no, no/yes, no/no) where merchants can still decide to authorize (accepting the risk) a transaction based on what it knows about its customer. Both sides however, still have veto power when the order is considered very suspicious.

RSA Security

Corporate Overview

Key Statistics

- Headquarters: Bedford, Massachusetts
- Size: 2.7K employees (Outseer division 200)

Key Dates

- 1982 – Founded
- 2006 – Acquired by EMC
- 2011 – SecurID breach via an attack on its 2-factor auth product
- 2017 – EMC acquired by Dell Technologies
- 2020 – Dell announced sale of RSA to Symphony Technology Group for $2.075b

Product Offerings

- Outseer 3-D Secure
- Outseer Fraud Manager
- Outseer Fraud Action

Approach

For financial institutions that need to offer additional cardholder protection and fraud management tools, RSA enables issuers and merchants to provide a consistent, secure online shopping experience for cardholders while reducing chargeback losses. This is made possible with:

- **Outseer Risk Engine.** evaluates txns in real-time with over 100 indicators.
- **Pattern Recognition Analytics.** Powered by a Bayesian analytical model.
- **Outseer eFraudNetwork.** Provide collective fraud intelligence to proactively identify and track fraudulent profiles, patterns and behaviors across over 150 countries.

Commentary

Outseer claims their Risk Engine is far more superior than others in the market, and we have quantifiers to prove it. The Risk Engine drives industry leading fraud detection rates and low false positive rates.

Outseer has little to no capabilities that can compete with predictive neural network model from other competitors that enable real-time learning and scoring. Sources state RSA's risk engine is handled with batch updates, which leaves a window for fraud to pass through without being detected.

Competitors use neural network model, machine learning and artificial intelligence to learn from and adapt to fraud patterns in real-time. Outseer does not have a dynamic rules engine that works to quickly and accurately identify the risk of a transaction in order to take immediate action on that transaction and close the window of vulnerability.

Outseer states they have more fraud data intelligence via their eFraudNetwork, containing ½ billion devices, 250m users and thousands of customers.

Outseer does have a large network of data; however, however much of this data is irrelevant to the data that banks need to reduce 3-D Secure fraud losses and chargebacks. Updates to the model score are not reflected in real-time which means that real value can only be received if fraud case mangers are marking fraud consistently.

Other competitors such as Cardinal Commerce and Arcot possess a larger network of global cardholders and real-time financial e-commerce authentication transaction data. For example, when fraud is identified on a card or device on Cardinal/Arcot's network, the model score is instantly updated for all the members and automated action is taken to stop the fraud on the very next transaction attempt from that card or device.

Major customer for RSA in UK are Lloyds and Barclays

Broadcom (Arcot)

Corporate Overview

Key Statistics

- Headquarters: San Jose, CA
- Size: 200 employees (Arcot division)

Key Dates

- Co-created 3DS with Visa earlu 2000's
- CA Technologies acquired Arcot in 2010
- Broadcom acquired CA Technologies (inc. Arcot) in Nov 2018

Product Offerings

- Arcot for Banking (Payment Security Suite)
- Arcot for Merchants
- Risk Analytics Network

Approach

Arcot has focused traditionally on the issuer side authentication channel, whilst Cardinal Commerce has been dominant on the merchant side. Arcot's current focus is to leverage their fraud data model to provide solutions to both issuer and merchant. The Arcot for Merchant solution was launched to .

In 2019 Broadcom created the Arcot Payment Security Division (PSD) headed by a new GM reporting into the Broadcom CEO. This is in response to Broadcom's potential to drive Arcot into a billion-dollar franchise.

Commentary

Arcot current strategy

The creation of PSD has seen a shift in how Arcot is managing their client base. Out of there 200 customers, only the top 25% made 80% of the revenue so they have segmented their customer base.

Since Sept 2019 the only commercial offering Arcot is position to the market is Arcot Unlimited (AU). This is one fixed charge over 12/24/36 months where the customer has unlimited consumption of all Payment Security services. The entry point for AU is $500k p.a.

The bottom 150 customers that provide Broadcom with < $500k p.a. in revenue are being pressured to move to AU. This means some customers are being asked to pay in excess of three times they were paying previously alienated a number of customers.

With Arcot now focusing on their top 50 customers there is opportunity for other ACS vendors to focus on this customer set.

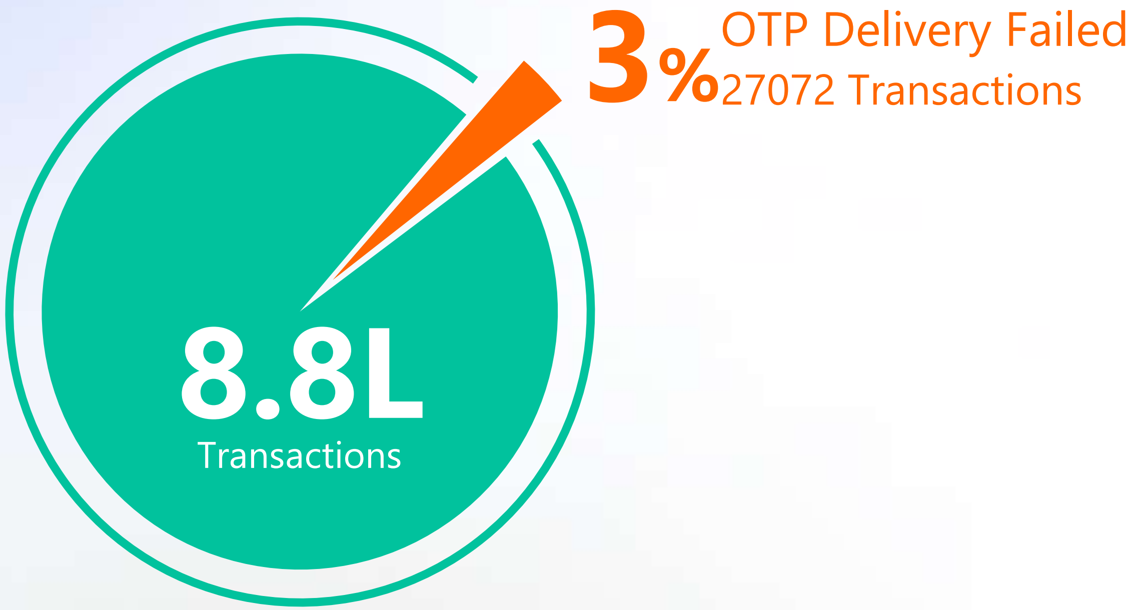
Major bank issuing customers are HSBC, RBS, Santander and Nationwide

Major processing partnership include TSYS, Fiserv and FIS

wibmo
a PayU company

www.wibmo.com

Case Study : Beyond SMS Authentication



Data Source
Bank : Among the Top 5 private Indian Bank
Data : Feb 1-15th, 2023

Merchant A (Among the **Top 5 TPAPs**)

78K Transactions

3.3% OTP Delivery Failed
2.5k Transactions

Merchant B (Among the **Top Telecom Providers**)

10K Transactions

3.4% OTP Delivery Failed
0.3k Transactions

Highlights

Avg time spent in OTP attempt : ~ 40 sec
Avg SMS cost : ABC units

Road Ahead

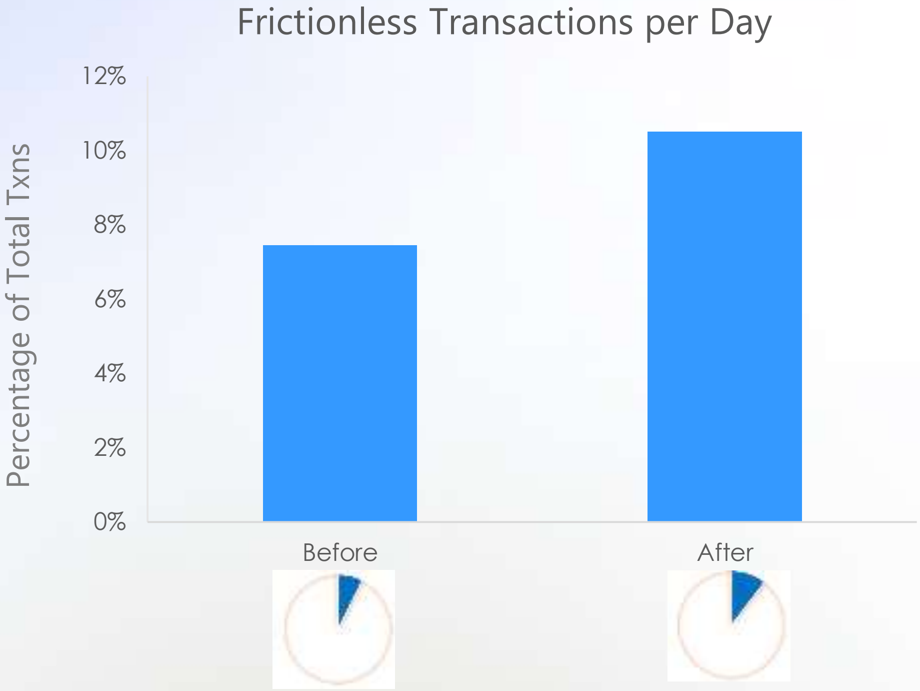
Risk Based Authentication : Trident
Multi-factor Authentication: Tridentity

Proposed Business Outcome

1.25% uptick as MDR charges
Reduction of SMS cost

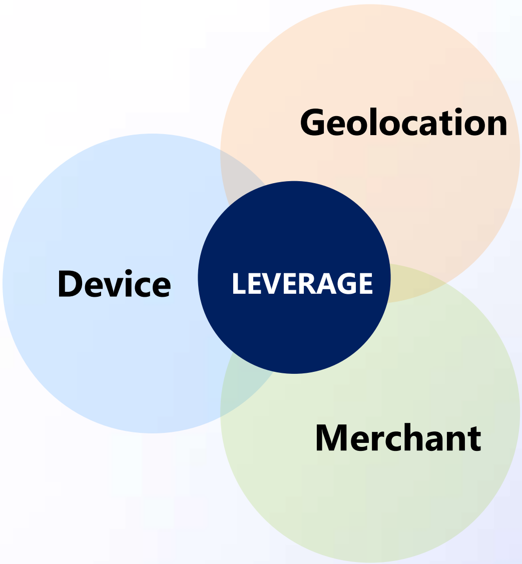
Case Study : FRICTIONLESS Payments (Major Bank : MEA region)

Highlights



↑3% Increase in **FRICTIONLESS** Transactions

↓ ⏱ Cards(customers) benefited with **REDUCED LATENCY**



Geolocation

Device

LEVERAGE

Merchant

Key Features

- ***Wibmo Device FingerprintJS*** to improve device id population (Incognito and iOS)
- Addition of corporate cards for complete frictionless payment experience

Road Ahead

AI/ML Model for issuer side Risk Based Authentication (RBA) to delight good customers with **frictionless payments experience**

Case Study : 3DS (Debit/Credit Cards)

68 Mn

Credit +
Debit Cards

Major Private Indian Bank

15 LAKHS

Average Daily Transactions

300+

Issuer Rules

500+

Transactions per Second

Sample Rules

- Previous transactions is low and next amount is high in 30 mins
- Last N days from particular MCC // Dormant users on particular MCC

Why Trident

SCALE

HDFC BANK
PayU
PAYZAPP
YES BANK
SBI card
kotak
HITACHI
Inspire the Next
SBI Payments
globalpayments
BOB Financial
Credit reimagined

Network
International Payment Solutions
HSBC
NIUM
BDO
بنك أبوظبي التجاري
ADCB

TECHNOLOGY

- **Scalable, Secure, and Reliable Cloud ready** deployment scoring 100% of the transactions in real time
- **REST-API driven seamless integration** with calling applications and third-party sources
- Fraud Analysis built on **customer-centric behaviour** using Advanced analytics & machine learning
- Monitor transactions against data points ranging across **user profiles, purchase patterns, sessions, device and transactions details**
- **Multi-Factor Authentication methods** ensuring the highest feasible seamless user-experience with Zero compromise on security and assurance.

BUSINESS

- **PA/PG Support**
  - International transactions
  - Domestic transactions
  - Tokenisation
  - UPI
  - AML

1+
BILLION
Transactions evaluated for risk annually

~10
Crores INR
Worth Fraud Amount saved Bank A in 2022

Fraud Scenarios, Modus Operandi & Prevention

Wallet

SCREEN SHARING APPs
Multiple transactions initiated from same IP/Device in short period of time

CASHBACK ABUSE
Most of the abuse registered names are Gibberish names, registered names for abuse cases are miscellaneous. Email/Name containing numbers in series .

SCREEN SHARING APPs

- Spoofed customer care details over the internet
- Request to install screen sharing app on the pretext of issue resolution through play store or link shared through SMS

PREVENTION : SAMPLE RULE

- Detect If the transaction is initiated from a device which has screen sharing enabled

UPI

SEEKING DONATION/SUPPORT IN THE NAME OF FAKE BENEFICIARIES
P2P transactions towards the beneficiary / VPA containing keywords like (Refund, Support, Army, Relief, Claim, Minister, reward, cashback)

QR CODE CLAIMING CASHBACK/OFFERS
Transactions towards QR with transaction notes with keywords like CASHBACK, WIN , OFFER

FAKE BENEFICIARIES

- Spoofed customer care details over the internet
- Request to install screen sharing app on the pretext of issue resolution through play store or link shared through SMS

PREVENTION : SAMPLE RULE

- Detect If the transaction is initiated towards a VPA beneficiary which contains suspicious keywords such as refund, support etc

Credit/Debit Cards

BURST OF TRANSACTIONS
Transactions initiated at High Velocity from a card, BIN or other relevant entities in a very short duration

SUSPICIOUS GEOGRAPHY MERCHANTS
Transactions initiated towards merchants which belong to blacklisted countries or suspicious cities

BURST OF TRANSACTIONS

- Spoofed customer care details over the internet
- Request to install screen sharing app on the pretext of issue resolution through play store or link shared through SMS

PREVENTION : SAMPLE RULE

- Detect If the number of transactions initiated from same card, BIN or other relevant entities in a period of time is greater than threshold

Dual Objective : SECURE & SEAMLESS Payments

WIBMO TRIDENT FRAUD AND RISK MANAGEMENT

Leveraging both transactional and non-transactional data elements for risk assessment based on rules and ML models for continuous monitoring against evolving fraud patterns

RISK CONTAINMENT

FRAUD RISK

- Monitoring
  - Financial Transactions
  - Non-Financial Transactions
- Prevent Fraud & Abuse
- Minimise Chargebacks

Holistic Risk based Approach & Adaptive Authentication

WIBMO TRIDENTITY MULTIFACTOR AUTHENTICATION SOLUTION

Multi-Factor Authentication methods ensuring the highest feasible seamless user-experience with Zero compromise on security and assurance.

CONVENIENCE & SPEED

EXTERNAL

- Seamless user experience
  - Authentication Methods
  - Quick Checkouts
- High Security & Assurance