The Importance of Creating a Physical and Digital Identity Strategy to combat Fraud

Jaime Rojas P.

Agenda

- Current Market Challenges
- Fraud and Identity Use Cases
- Capabilities of Fraud and Identity Solutions
- How to Create a Digital Strategy

REAL-TIME DECISIONS

INTEGRATION HUB

IMPROVED MERCHANT ONBOARDING

REDUCE CHARGEBACKS BY 70%

ONGOING TRANSACTION SCREENING

FRAUD STRATEGY

SIMPLE VIEW OF CUSTOMER

COMPLEX EVENT PROCESSING

INNOVATION

AGILITY

ADAPTIVE ANALYTICS

WORLDS LARGEST DIGITAL IDENTITY NETWORK

SIMPLE INTEGRATION AND LOW TCO

MACHINE LEARNING

COMPLIANCE RISK MITIGATION

E-KYC

STRONG DEVICE FINGERPRINT

Current Market Challenges

Increased fraud risks are top of mind for Consumers

~4.5 billion

digitally active consumers[2]

~10 billion

human digital authentications per day[3]

45%

of businesses reported that they fully understand the impact that fraud is having on their business.

93%

U.S. businesses have mid to high concern for fraud

~90%

businesses are prioritizing increasing digital acquisition and improving fraud protection

Customers expect Frictionless Access

The Digital World is Anonymous

Businesses need to safely grow

Current Market Challenges

Control Fraud Losses at Account Opening

Identity Theft Fraud and Synthetic Identity Fraud

Defend Against Account Takeover Fraud

Protection across all contact channels
(in branch, call center, website, mobile app)

Reduce the Customer Impact/ Positive Identification

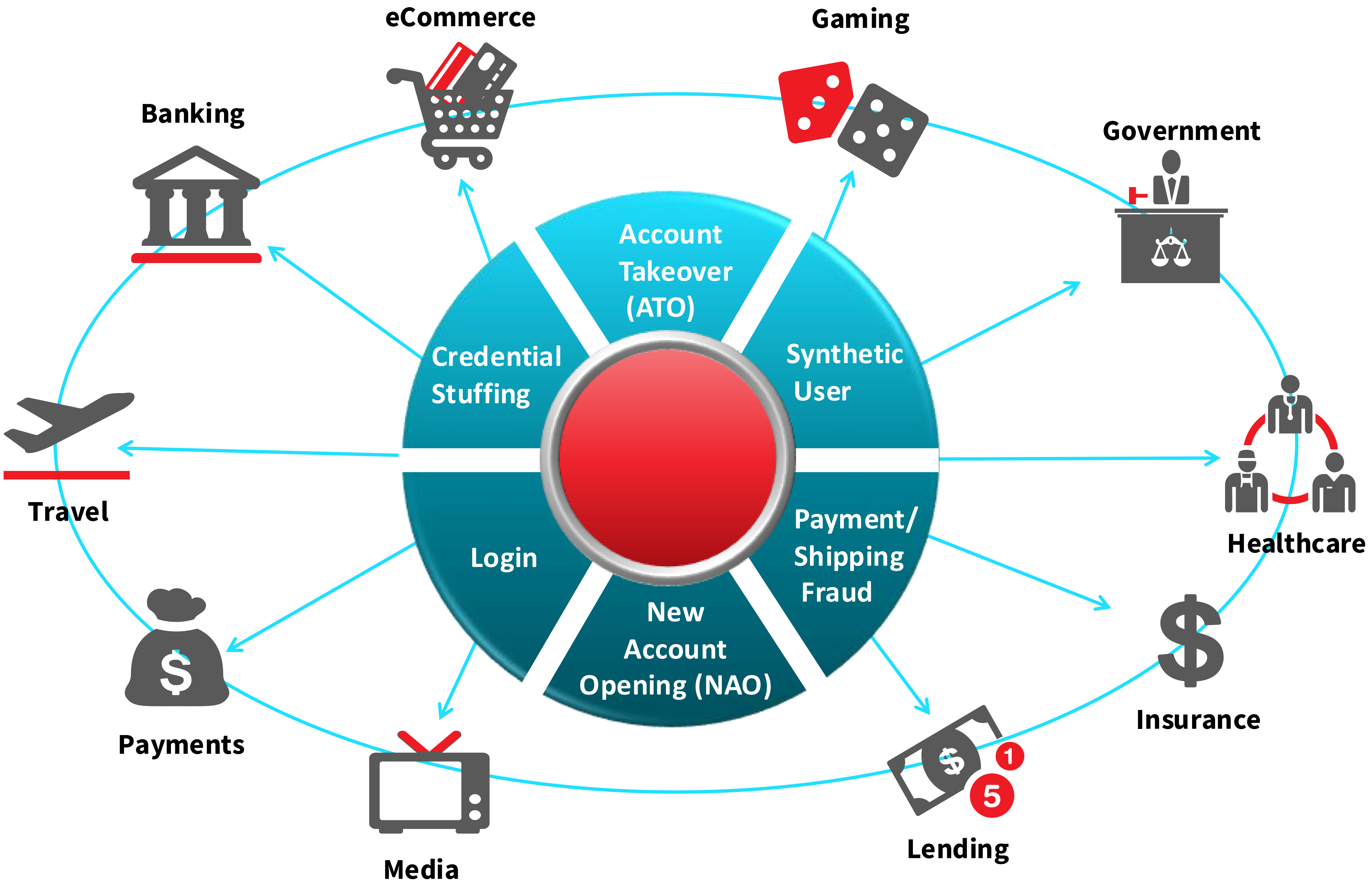
Less friction, more choice, passive approaches

Avoid Reputational Risk

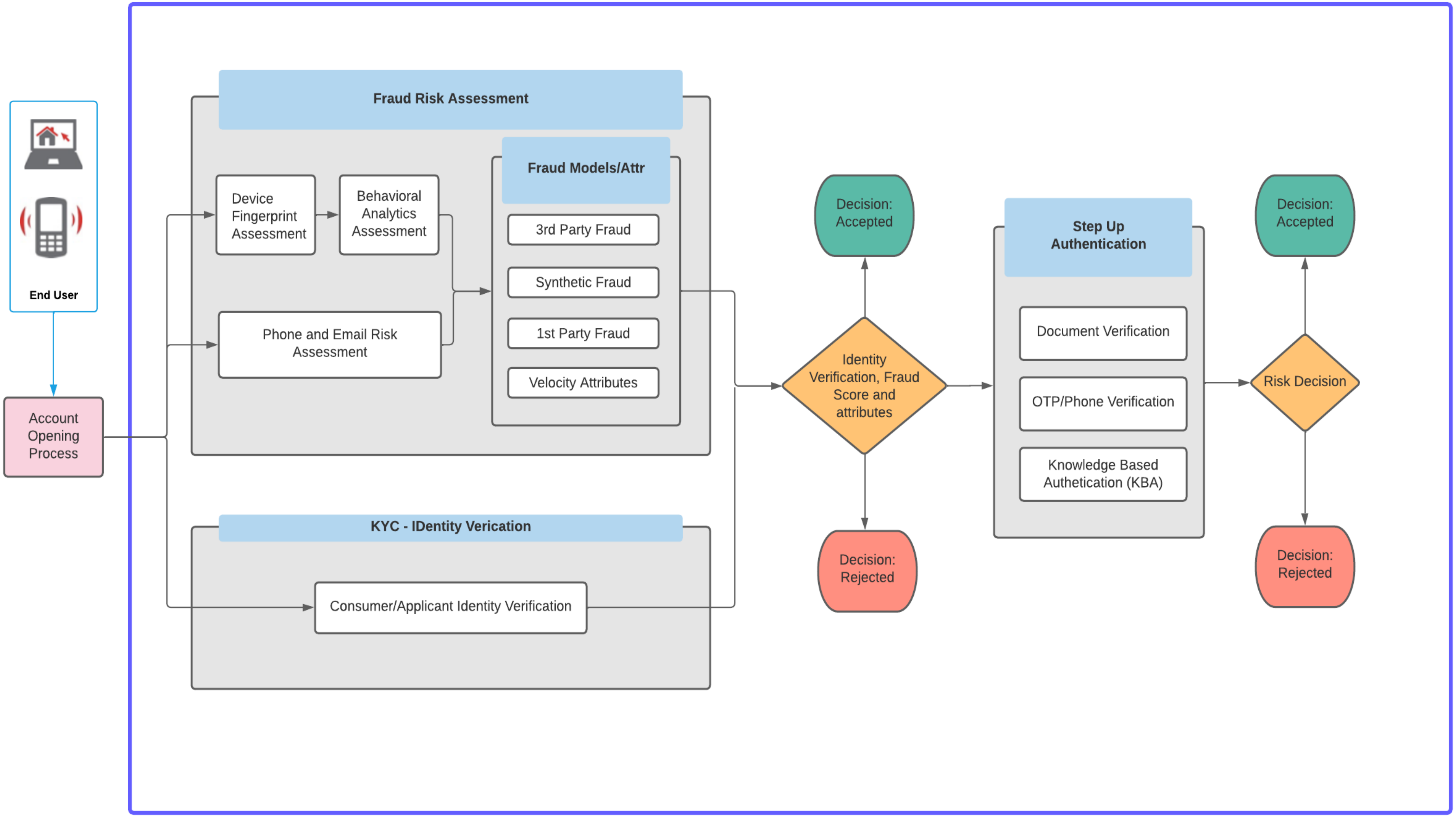
Supporting regulatory compliance and best practices
in fraud detection and identity management

Fraud and Identity Use Cases

Fraud and Identity Use Cases Use

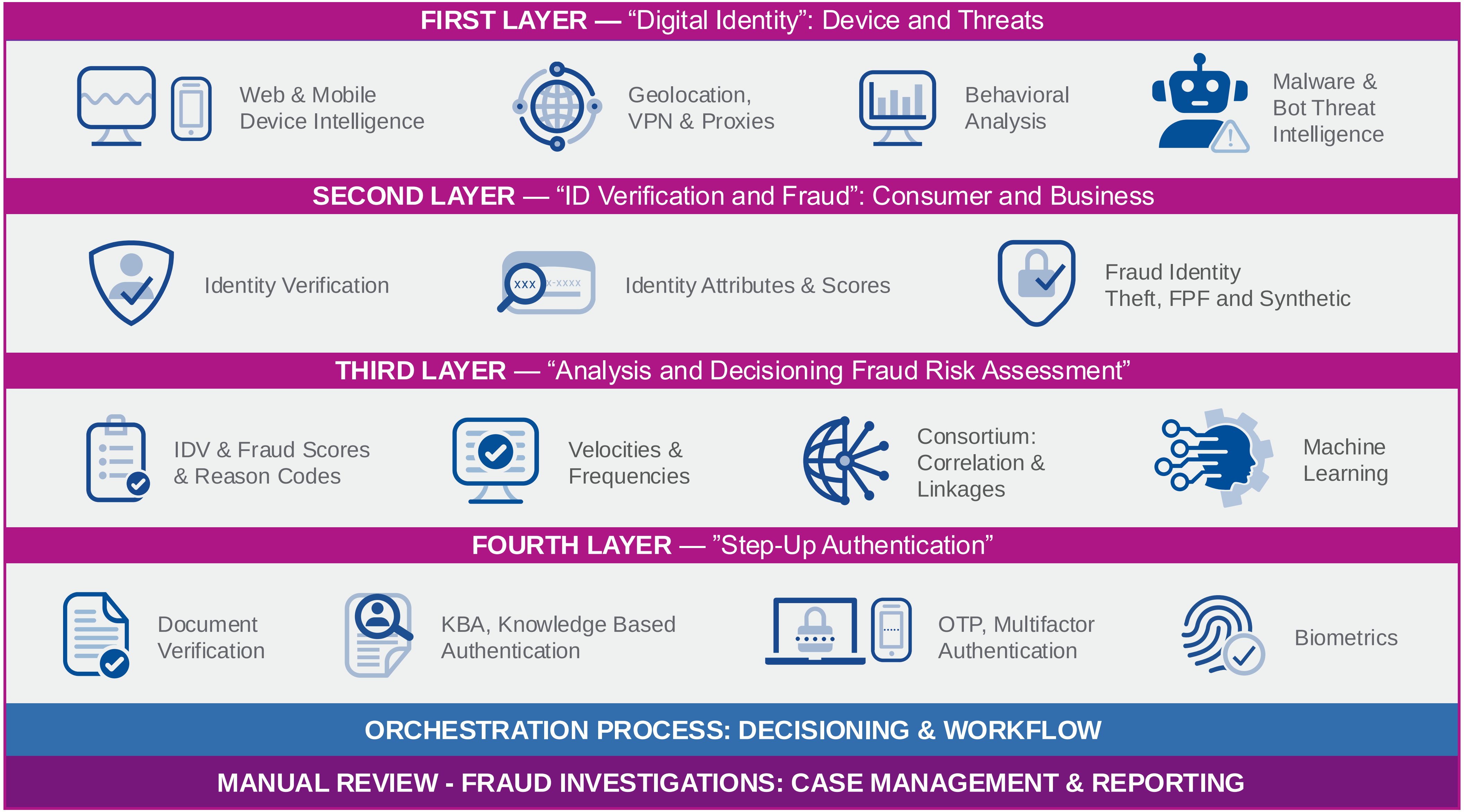


NAO Use Case - Fraud and Identity Solutions



Capabilities of Fraud and Identity Solutions

Your digital fraud prevention strategy ”standard”



FIRST LAYER — “Digital Identity”: Device and Threats

- Web & Mobile Device Intelligence
- Geolocation, VPN & Proxies
- Behavioral Analysis
- Malware & Bot Threat Intelligence

SECOND LAYER — “ID Verification and Fraud”: Consumer and Business

- Identity Verification
- Identity Attributes & Scores
- Fraud Identity Theft, FPF and Synthetic

THIRD LAYER — “Analysis and Decisioning Fraud Risk Assessment”

- IDV & Fraud Scores & Reason Codes
- Velocities & Frequencies
- Consortium: Correlation & Linkages
- Machine Learning

FOURTH LAYER — ”Step-Up Authentication”

- Document Verification
- KBA, Knowledge Based Authentication
- OTP, Multifactor Authentication
- Biometrics

ORCHESTRATION PROCESS: DECISIONING & WORKFLOW

MANUAL REVIEW - FRAUD INVESTIGATIONS: CASE MANAGEMENT & REPORTING

Physical Identity fraud prevention for consumer

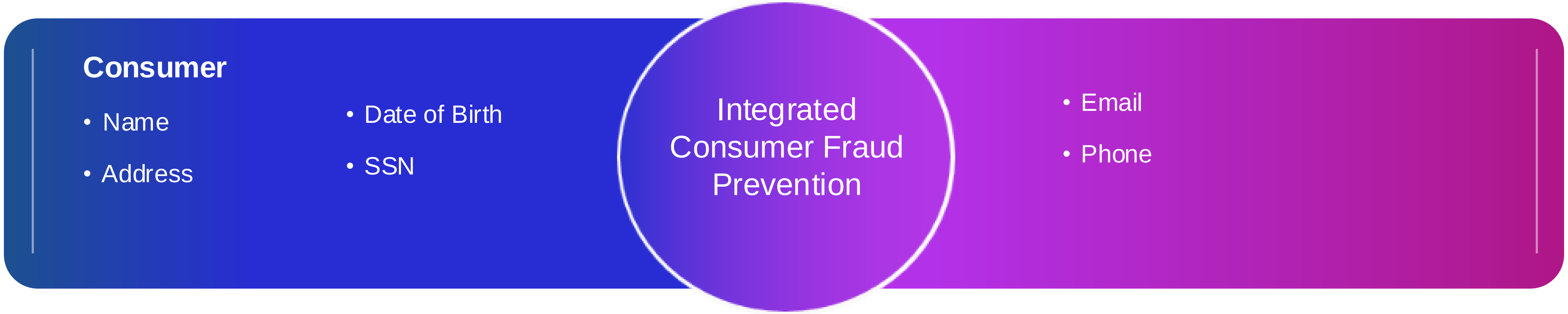
Know Your Customer **(KYC)**

Consumer identity insights + intelligence

- Consumer identity elements
- Fraud Risk Scores:
  - Identity Theft Fraud
  - Synthetic Fraud
  - First Part Fraud

- Email address risk
- Phone risk insights
- AML and watch list screening

- Increase Auto-Approval KYC
- Decrease Manual Review
- CX: good customer
- Friction risky customer



Consumer

- Name
- Address
- Date of Birth
- SSN

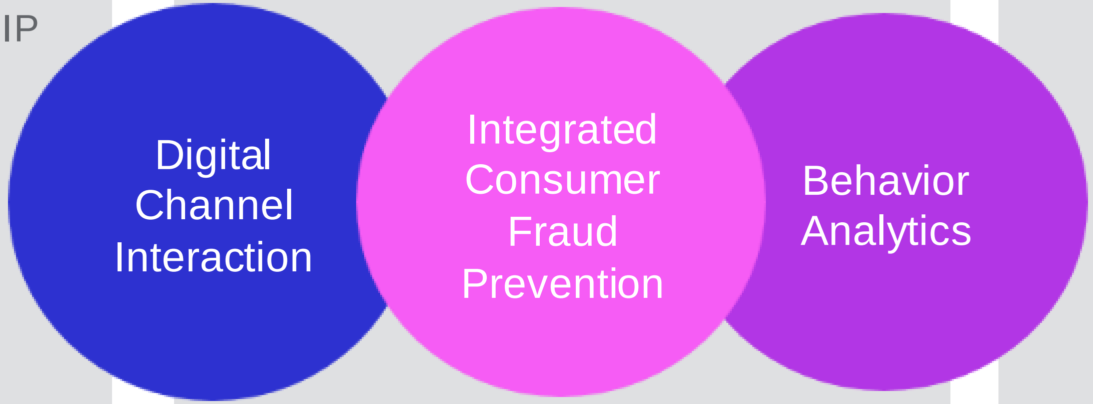
Integrated Consumer Fraud Prevention

- Email
- Phone

Digital Identity fraud prevention for consumers

Device insights + intelligence

- Location spoofing: VPN, Proxies, IP
- Device spoofing and anomalies
- Device ID persistence
- Malware and Man-in-the-Browser
- Consortium and Link Analysis


Digital Channel Interaction
Integrated Consumer Fraud Prevention
Behavior Analytics

Behavior insights + intelligence

- Behavioral Signals
  - ○ Typing speed
  - ○ Copy & paste
  - ○ Time spent on form
  - ○ Number of change/time
- Bots and AI Attacks
- Data Familiarity
- Combine with ML model
- Consortium

Fraud and Identity Solutions - Use Cases

New Account Opening (NAO)

Client Problems or Pains:

- Location Spoofing – Fraudster uses VPNs or proxies to manipulate location.
- Device Spoofing – Fraudster uses tools to alter several device markers used by OS, user-agent, browser, screen, etc.
- ID Verification and Identity theft

Solution Capabilities:

- VPN, DNS server IP, and IP detection
- Device ID persistence
- Business, guarantor, consumer verification
- 3P Fraud and Synthetic detection, ML
- Device Fingerprinting
- Behavioral Analytics
- Link Analysis
- Consortium

Account Takeover (ATO)

Client Problems or Pains:

- Bot Attacks – Used to execute large-scale Bot attacks on a login page.
- Man-In-The-Browser malware attacks – Are executed by client-side trojans, to manipulate page content and scripts to obtain personal data:
  - ✓ login credentials,
  - ✓ credit card details,
  - ✓ addresses, and other personal information.

Solution Capabilities:

- VM, RATs, VPN/proxy detection
- Identify device anomalies and malware attacks
- Detect high-velocity traffic frequencies and email
- Device Fingerprinting
- Behavioral Analytics
- Link Analysis
- Consortium

How to Create a Digital Strategy

Digital Transformation and Customer Experience

Clients’ Pain Points

Case Management

“Respond to common fraud patterns …”

Risk Score Engine

“The solution must be capable of detecting, flag and manage suspicious activities…”

ID Verification Tools

“Authentication for all the products and services provided across all branches and channels…”

Dashboard, Reports

“It is required Reports, Dashboard, and Audit Trail...”

Self-Services Center Console

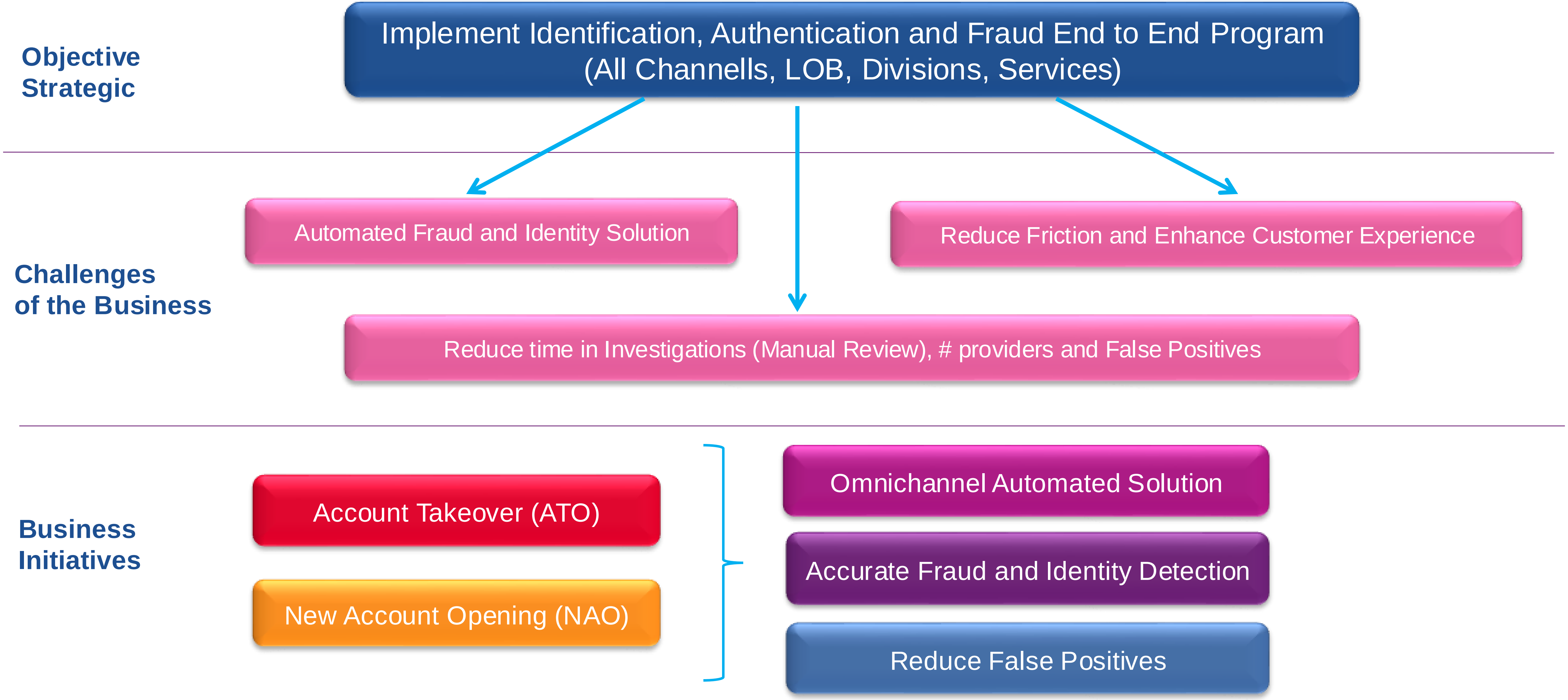
“Rules Improvement, ML Models, and Monitoring…”

Data Management

“Available data to integrate with our systems...”

DIRECT | BRANCH OFFICES | PHONE | WEB | MOBILE | SOCIAL

Digital Strategy



Objective Strategic

Implement Identification, Authentication and Fraud End to End Program (All Channells, LOB, Divisions, Services)

Challenges of the Business

Automated Fraud and Identity Solution

Reduce Friction and Enhance Customer Experience

Reduce time in Investigations (Manual Review), # providers and False Positives

Business Initiatives

Account Takeover (ATO)

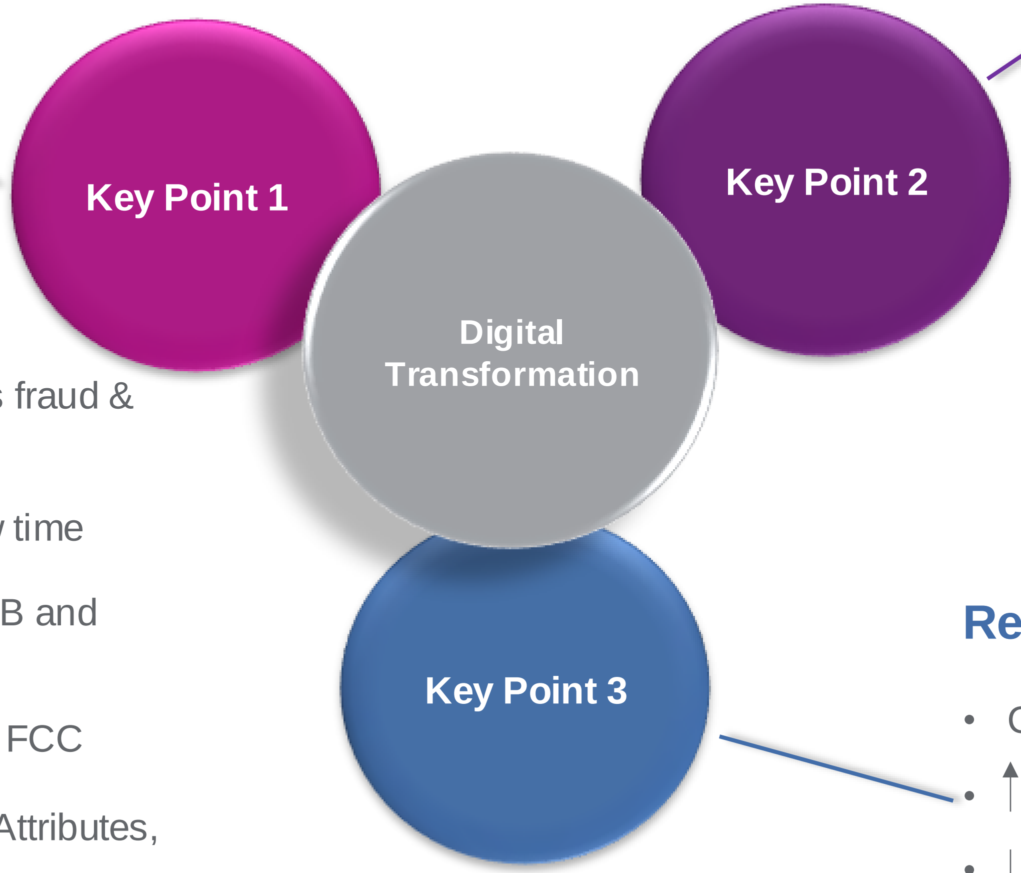
New Account Opening (NAO)

Omnichannel Automated Solution

Accurate Fraud and Identity Detection

Reduce False Positives

Key Points Solution - Digital Transformation



Omnichannel Automated Solution:

- Improve CX, monitoring, and detection of omnichannel
- Digital and Physical channels fraud & Identity Risk Assessment
- Reduce Fraud Analyst review time
- Screening compliance for KYB and KYC
- Detect Risk Locations – AML FCC
- Decisioning: overall Results, Attributes, Reason Codes and Scores

Accurate Fraud and Identity Detection:

- Solution, verify Business, Owners/Applicants, and Consumer
- Strong Fraud detection: FPF, 3PF, Synthetic.
- Strong Digital fraud detection (Devices, IPs, Bots, AI Fraud attacks, etc.)
- 360-degree view of Digital and Physical Identity.

Reduce False Positives:

- Customized strategies and Workflows
- ↑ Auto-approval KYB, KYC + Customer Experience
- ↓ False Positives, Friction, MR, and # Providers
- ↑ Fraud Capture Rate
- ↓ Opex, Operational Costs and time

Thank you