Transmit Security

Move Fast. Be Secure. Never Compromise

Paolo Fabbri
Transmit Security Ltd – Sales Lead Italy
paolo.fabbri@transmitsecurity.com

We imagine a world where companies are not forced to compromise between Security and exceptional Customer Experience

Mickey Boodaei - CEO and Co-Founder, Transmit Security

Introducing Transmit Security

LAUNCHED IN

2016

By Serial Entrepreneurs

Mickey Boodaei and Rakesh Loonkar

300+

Employees Worldwide

HEADQUARTERED

in Tel Aviv & Boston

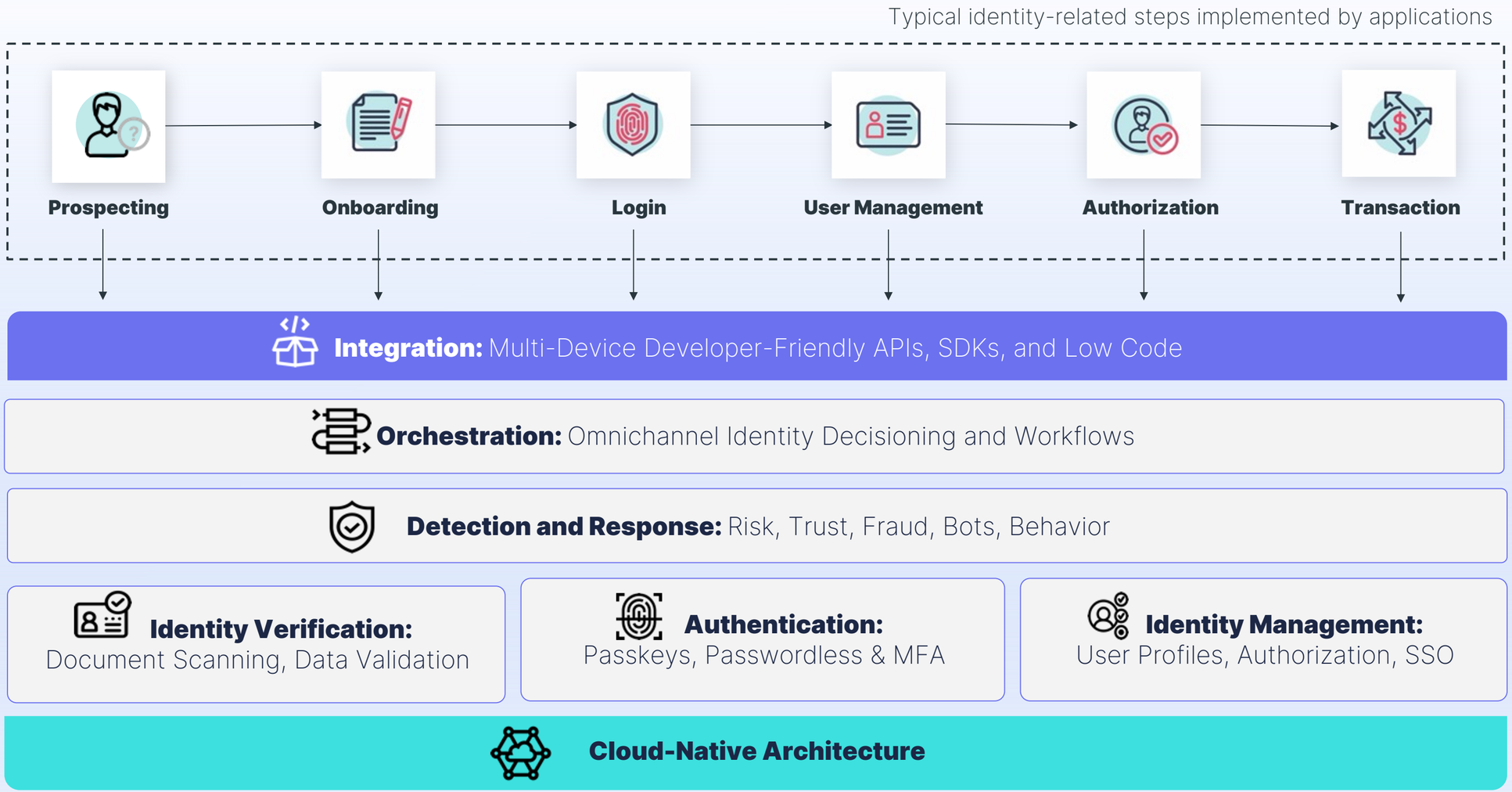
1+ Billion

Identities Managed

Industry Leadership

- FIDO Alliance Member
- Top 10 Most Innovative Security Companies of 2022 - Fast Company
- Only Identity “Market Leader” Across 3 KuppingerCole Leadership reports
- Cool Vendor - Gartner 2020
- Winner - Deloitte Fast 500

Transmit Security Platform

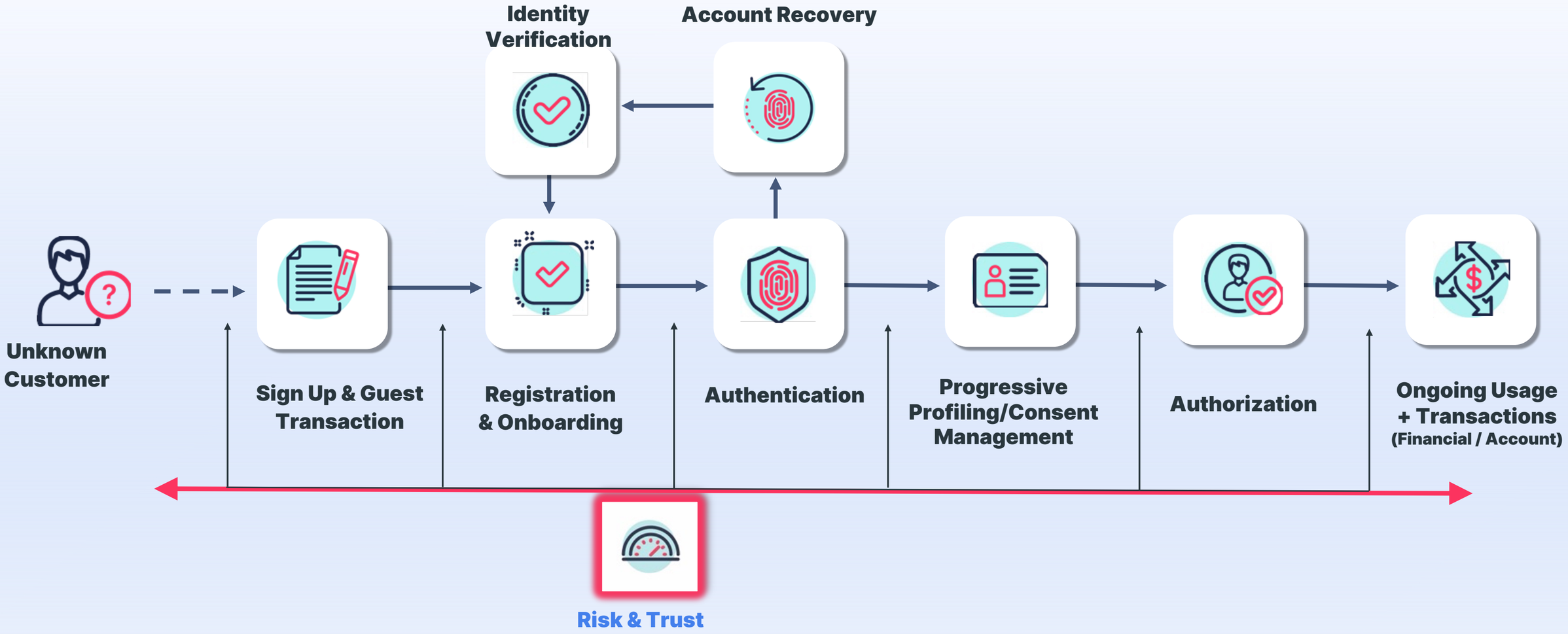


End to End Frauds Architecture

Welcome your credible users, keep the bad people out

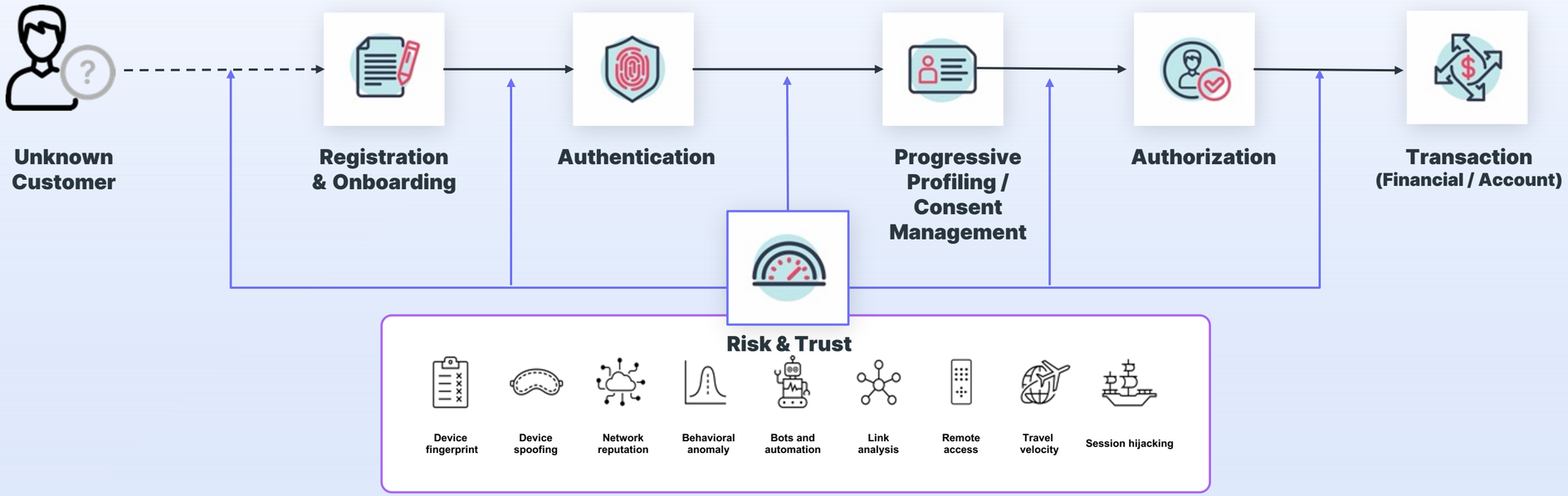
transmit security

Customer Journey on channels



Continuous Risk and Trust Assessment

Detect early, keep detecting

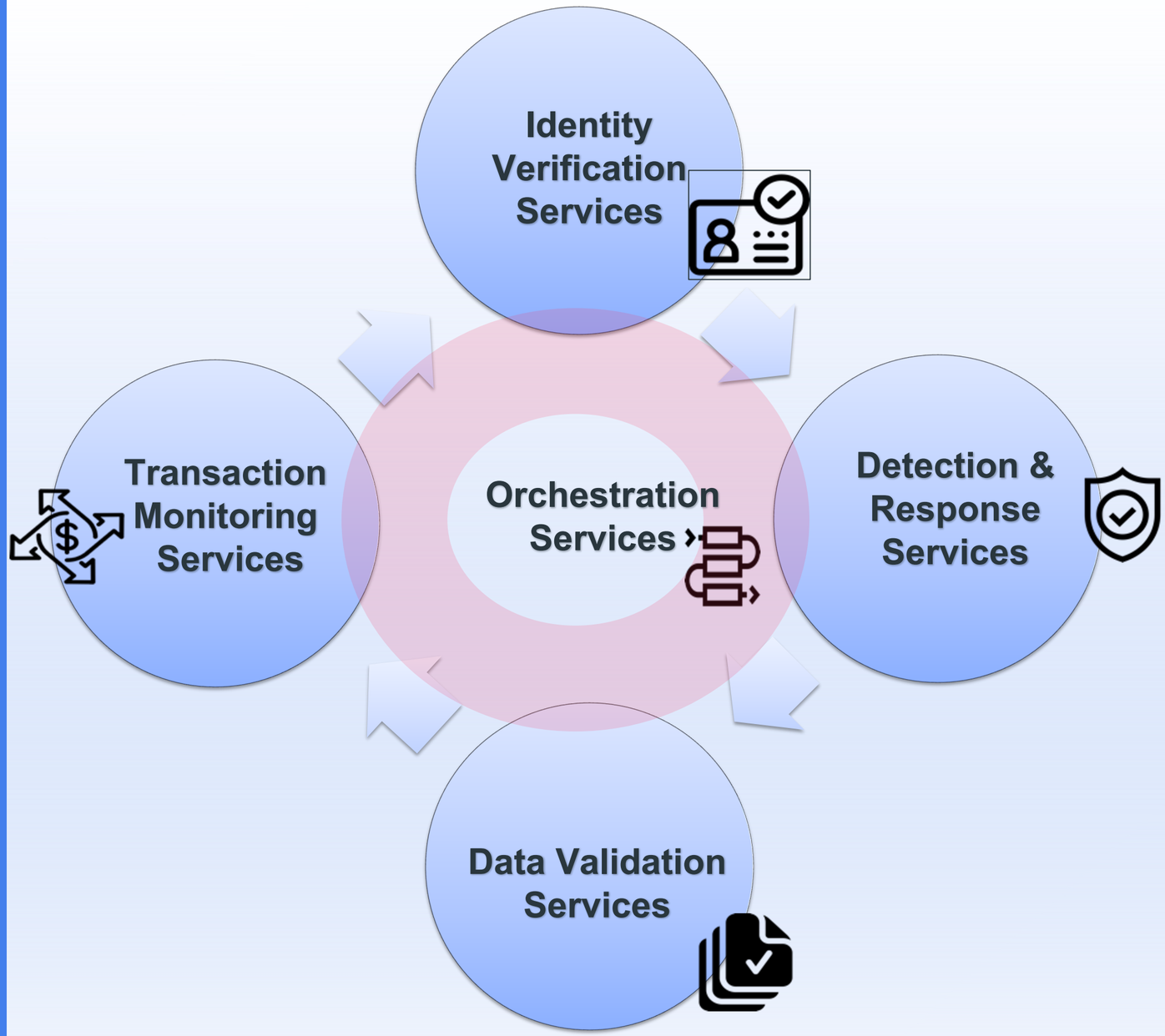


Provide an immediate recommendation, at real time, at every risk moment

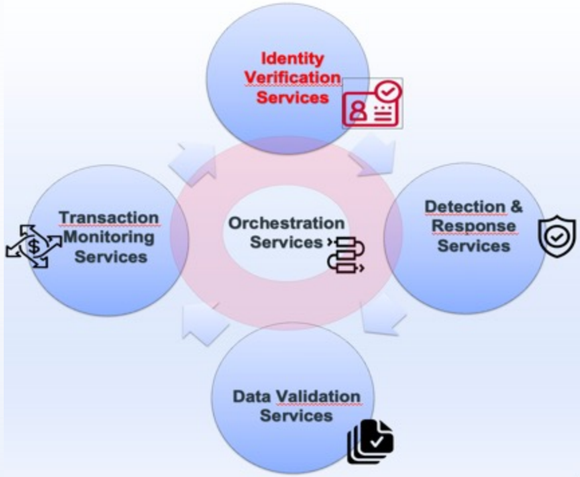
Base on recent threats, patterns, and rich context - device, network, behavior, account changes, ...

Frauds Prevention & Detection

End to End



Identity Verification



- **Document Verification**
  - highly accurate verification for many types of documents through powerful OCR tool
  - document verification for non-tampering
- **Continuous context risk assestment** during onboarding's phases to prevent risks

Uncompromising Accuracy in ID Verification

Hundreds of checks on the document within only a few seconds

Portrait
- Photo Background
- Edges/Corners
- Photo Dimensions
- Color
- Photo Integration technology (glued,stamped, etc.)

Liveness
- Device Screen
- Printed cutout
- Printed data placements
- Holographic overlays

Document Structure
- Layout Mismatches
- Colors
- Corners
- Hole punch

Fonts
- Font Style/Family
- Font Color
- Formatting

NFC
- Passive authentication
- Active authentication
- Data comparison

Security Features
- Holograms/DOVID
- Embossing
- Ghost images
- 50+ additional checks

MRZ
- Data Validity
- Data comparison
- Check Digits/Checksum

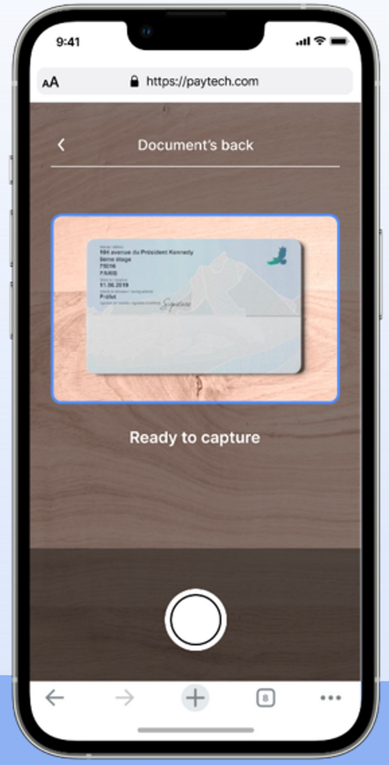
Template Mismatch
- Issue Date
- Data Validity
- Format Validity

Barcode (PDF417)
- Data Validity
- Data comparison
- Data format
- Data Structure

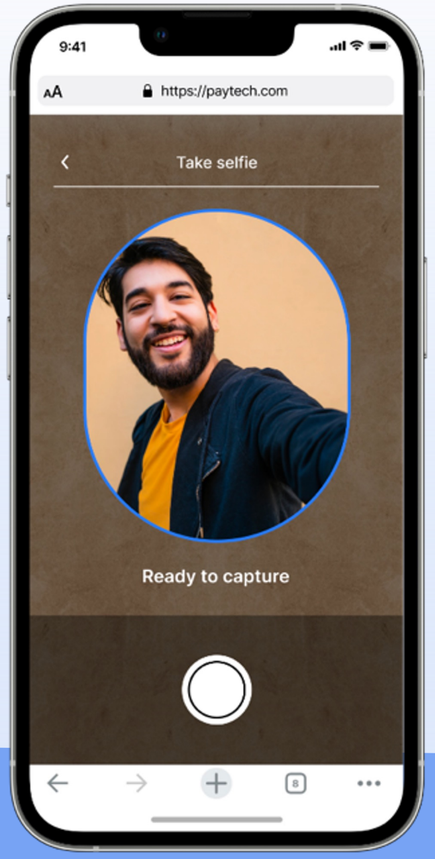
transmit security

ID Verification Process

Document's Front



Document's Back



Liveness + Face match

100+ risk detection mechanisms continuously running in the background

Identity Verification : Expected Business Outcomes

Reduction of false positives and false negatives by

90%

Reduce new account operational costs by

80%

Comply with

KYC/AML

Regulations

Reduce identity takeover losses by

80% or more

Reduce account opening dropout rates by

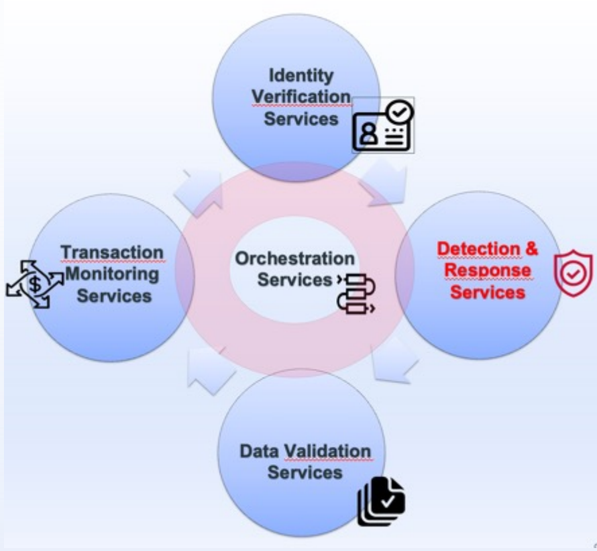
50% or more

Reduction in

complexity and costs

from vendor consolidation

Detection & Response



- **Advanced telemetry** with over **100 controls RELATED**:
  - Context
  - Device
  - network, bot detection behavior, 360-degree authentication methods during all stages of customer journey
- **Continuous 360-degree view** and analysis at all stages of the customer's journey
- **Native integration** with Identity Verification
- Fast and Flexible multi-method integration adaptable to any onboarding flow

Telemetry Types (examples from hundreds)

Telemetry streams from each interaction are correlated and analyzed in real time while adding key signals to the user's profile

Device

- Browser language, cookies, plugins
- OS settings, patches, drivers
- Model, Carrier
- GPU, CPU, codecs
- App & File Inventory

Account Changes

- Address/Contact
- 2FA setting
- Password change/reset
- New device registered
- Linked financial accounts

Behavioral Biometrics

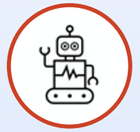
- Mousing patterns, velocity
- Touchscreen patterns
- Keystroke dynamics
- Movement consistency
- Input method

Global Intelligence

- Device reputation
- IP reputation
- Data center reputation

App Activity

- UI click locations
- Page sequences
- Action patterns
- Usage times
- Transaction actions



Bot Activity

- Credential stuffing
- Automation frameworks detection
- High velocity rates (IP, device, ...)
- Text Input behavior
- Mouse/Touch movements

Network

- IP / IP Location
- User agent
- Data center
- Proxies
- VPN

Authentication

- For initial logins, 2FA, step-ups
- Authenticator method, tool
- Pass/fail/abandon
- Velocity

User Profiling

- Account changes
- Trusted devices
- Common locations, ASNs, time zones
- Impossible travel
- Behavioral analytics
- Credentials Input methods & Keystrokes dynamics

Telemetry types are selected by threat research and data science teams based on proven ability to accurately detect risk and trust signals across a wide range of legitimate and fraudulent user scenarios

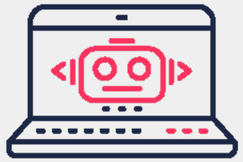
Detection & Response: Business Outcomes (Example)

Reduce false positives
and false negatives by

90%

Reduce new account
operational costs by

80%



Reduce bots and automated attacks
by

98%

Improve device fingerprinting
accuracy to

99.7% or better

Reduce friction, MFA
and CAPTCHA challenges by

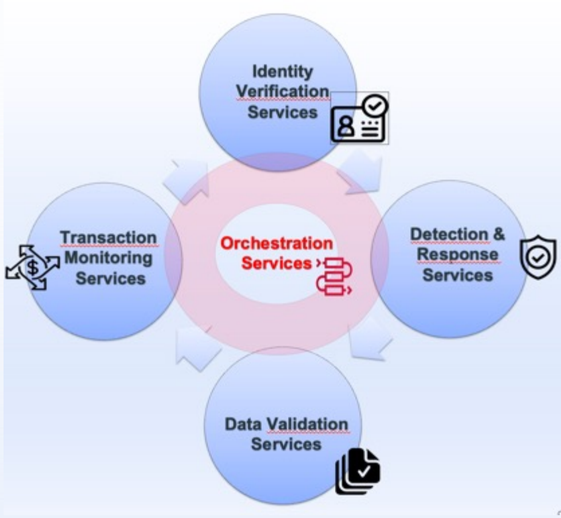
80% or more

Reduce

complexity and costs

from vendor consolidation

Orchestration



Fraud orchestration refers to the process of coordinating various tools, technologies, and resources to detect, investigate, and respond to fraudulent activities effectively.

The primary goals of fraud orchestration are to enhance an organization's ability to :

- **prevent,** detect, and mitigate fraudulent activities **cross any business process**
- **minimizing** operational **costs** and reducing risks

- **Early Detection**: Identify fraudulent activities as early as possible to minimize financial losses and reputational damage. This involves setting up real-time monitoring and alerting systems.
- **Real-Time Responses**: Enable real-time decision-making and responses to detected fraud, such as blocking transactions, freezing accounts, or initiating further investigation.
- **Continuous Improvement:** Use data analytics and machine learning to continuously improve fraud detection models and strategies based on evolving fraud patterns.
- **Single Point of control** cross any business process (Onboarding – Detection- Changes)
- **Cross-Channel and Cross-Product Visibility**: Gain a comprehensive view of fraud activities across different channels (e.g., online, mobile, in-person) and various products or services offered by the organization.
- **Easy integration** with multiple detection services part or not part of Transmit porfolio

transmit security

RIGHT Orchestration Architecture on Frauds strategy enables :

- ✓ **360° reuse of services** in every step of Detection & Prevention activities
- ✓ Makes detection **faster, efficient and effective**
- ✓ **Reduce costs** to **implement and evolve** detections mechanisms and mitigation solutions
- ✓ **Data Validation** Easy interfacing and use of Data Providers (third-party systems) in order to validate personal informtions

Transaction Montoring

Detection types

- Velocity checks of payee device
- Velocity checks of payer device
- Velocity checks of payer network
- Anomalous volume traffic based on payee and payer profiles
- Anomalous amount based on payee and payer profiles
- ...

Data points (outgoing and incoming transactions)

- Payer
  - Name /Branch ID / Account number
- Payee
  - Name / Bank ID / Branch ID
  - Account number / Transaction reasonTransaction date
- Amount
- Currency

Transaction Montoring

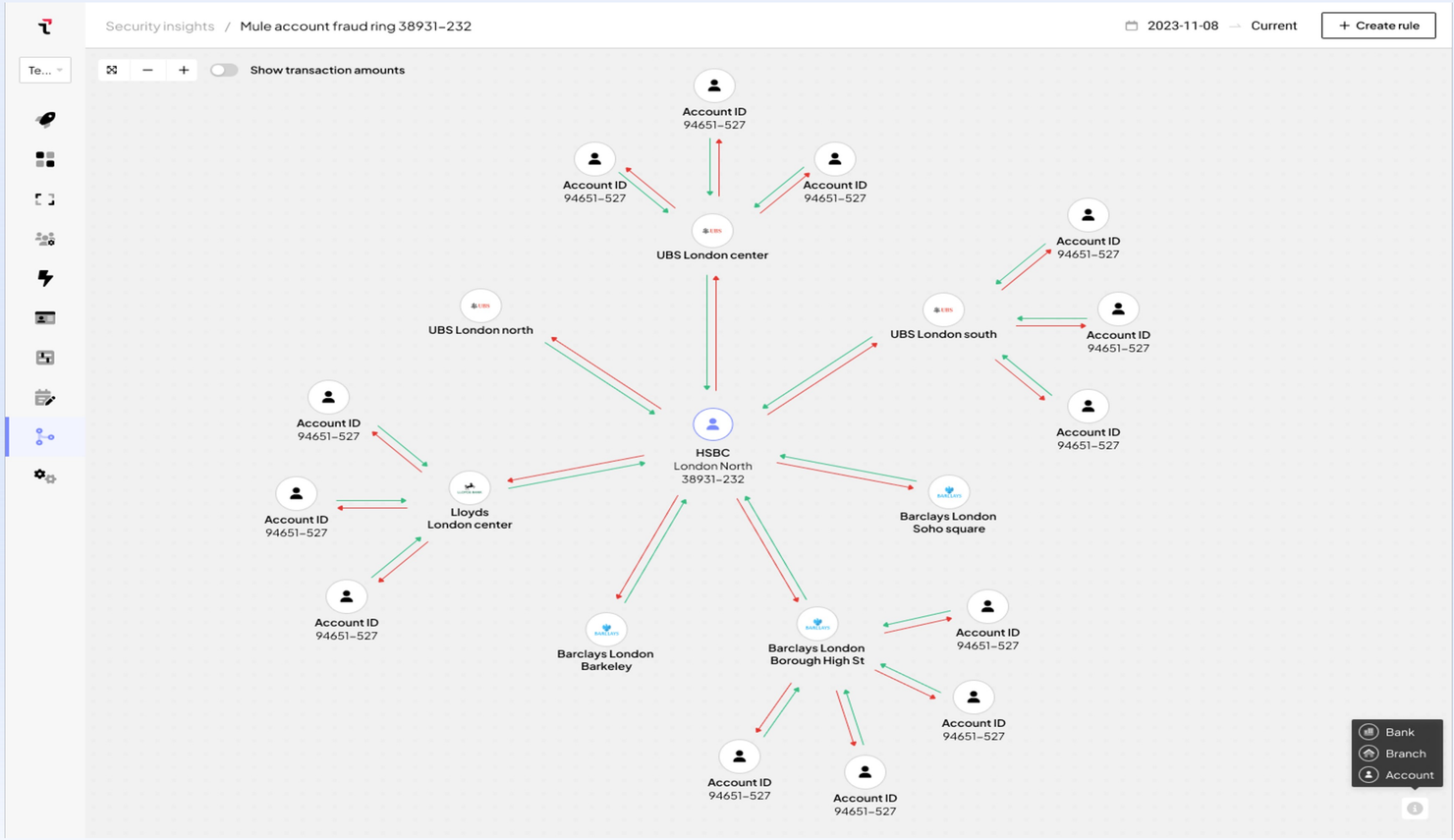
Social engineering fraud detection – Intelligent Chatbot

- The platform also includes **a Chatbot assistant able** , where a potential fraud is intercepted due to behavior not in line with the customer's profile and the history of operations, **to** :
  - open a contextual communication channel with the customer
  - highlight potential risks
  - interact with the customer through questions and answers aimed at prevent frauds
- Thanks to this approach:
  - WE SUPPORT the customer better during the transaction phases
  - WE PREVENT attempted fraud in the most critical phases of the transaction
  - WE RECORD the interaction with the customer on the specific case in the event of a claim
  - WE GET an additional risk assessment through customer interaction

Transaction Montoring

Post-detection analysis

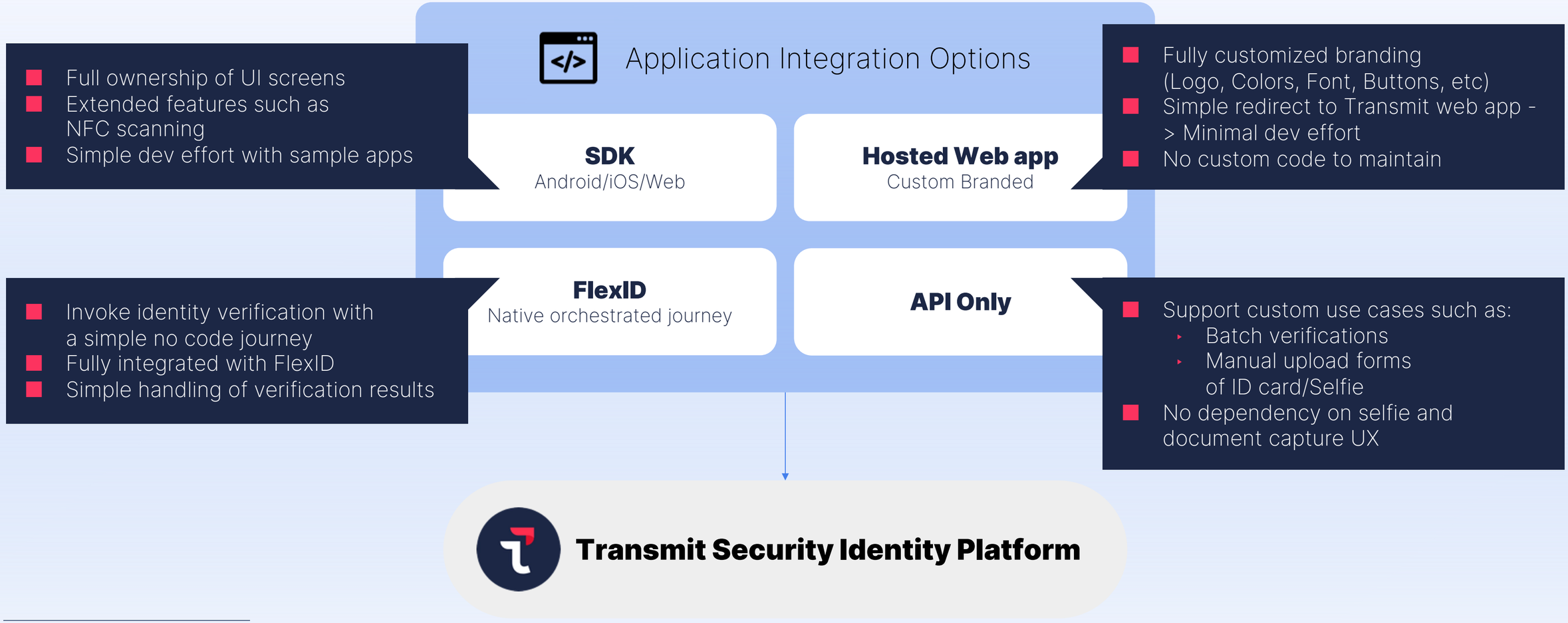
- Link analysis between banks and accounts
- Offline risk evaluation of transactions and account to match with known fraud/money laundering/money mule patterns



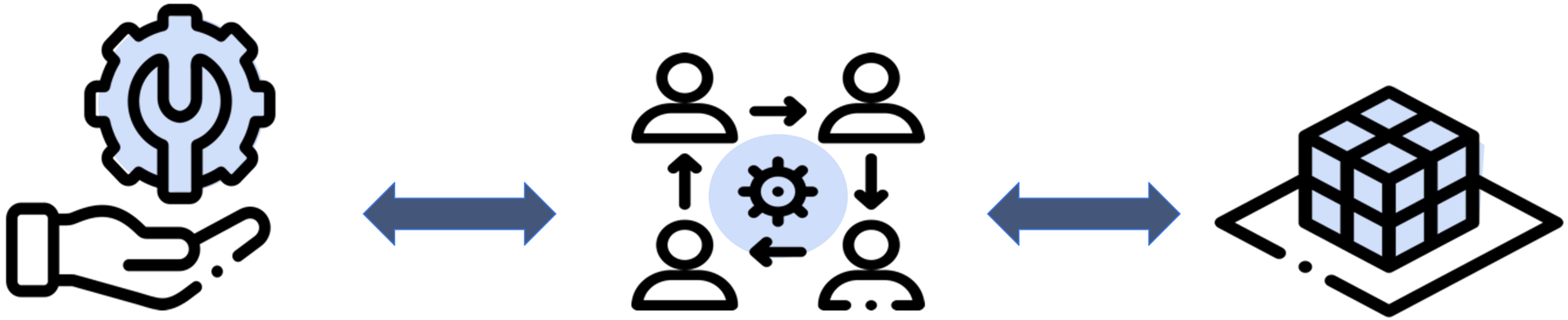
transmit security

Options for quick and efficient implementation

Quick time to value



Transmit Fraud Approach and Vision



Technology **People** **Process**

- Analyze the "As is" gaps with market counterparts (Customers and Partners), Identify challenges, inefficiencies and opportunities to create value.
- Define a mutual value plan to promote a multi-year evaluation program based on: value measurement, mutual challenges, common and measurable OBJECTIVES
- collect new requirements and for the evolution of Transmit services

In summary: Transmit’s distinctive points

- ✓ **Unique, powerful,** versatile fraud **Orchestration Engine** able to of manage complex correlations and ready to reactin "real time"

- A very **accurate Detection system** (best in class) able to collect detailed risk information

- A **Transaction Monitor** system supported by an **AI** system capable of reacting to risks in a responsive manner (e.g. Intelligent Chatbot)

- **Enterprise architecture:**
  - **easy to integrate** and evolve
  - Base on standards
  - without technical constraints

THANK YOU