InAuth

Digital Intelligence Experts

CONTENTS

01 Fighting Fraud with Digital Intelligence

02 Technology

03 Why InAuth

01

Fighting Fraud with Digital Intelligence

Fraud Follows the **Money**

NEW ACCOUNT OPENING AND APPLICATION FRAUD

Fraudsters open an account with a true or fake identity

PAYMENTS FRAUD

Fraudsters use compromised card or account credentials to make purchases or send money

ACCOUNT TAKEOVER FRAUD

Fraudsters obtain access to a legitimate user's account

The number of data records stolen, lost, or exposed worldwide hit **2.6 billion** in 2017

-Gemalto, April 2018

Digital Fraud Tactics

- VELOCITY ATTACKS
- BOT ATTACKS
- MALWARE / CRIMEWARE
- CLOAKED ROOT / HIDDEN JAILBREAK
- TAMPERING
- MAN-IN-THE-MIDDLE
- SPOOFING TOOLS AND EMULATORS
- INSECURE COMMUNICATIONS

Consequences

$71B
Amount merchants will lose globally to card-not-present fraud in the next five years
- JUNIPER, JUNE 2017

$118B
Annual decline amount due to incorrect transaction declines
- JAVELIN, AUG 2015

$5.1B
Total account takeover losses in 2017, a 120% increase from 2016
- JAVELIN, 2017

81%
CNP fraud more likely than point of sale fraud
- JAVELIN, 2017

52%
False positive rate for merchants
- ETHOCA, APRIL 2017

1.5M
Victims of existing account fraud had an intermediary account opened in their name first
- JAVELIN, 2017

DIGITAL INTELLIGENCE
Key to Better Fraud Prevention

InAuth analyzes **devices** and **associated identities** to ensure trust with those interacting within your digital channels, helping your business

- VERIFY IDENTITY
- ASSESS AND MITIGATE RISK
- OPTIMIZE THE CUSTOMER EXPERIENCE
- IMPROVE OPERATING PROCESSES & REDUCE COST

02 Technology

The InAuth Security Platform

Device intelligence and risk assessment solution to more consistently identify and better validate the trustworthiness of every device transacting within your digital channels

InMobile®

Enhanced authentication, device integrity screening, and cybersecurity mechanisms for devices transacting through mobile applications

InBrowser®

Best-in-class technology to authenticate any web-connected device with a browser through next-generation fingerprinting

InRisk®

Device analysis and risk assessment system with configurable business rules and device confidence scoring

InAuth Security Platform

Delivering **more data points** for device identification and risk analysis

DEVICE ID

OPERATING SYSTEM

LOCATION

IP

DEVICE CONFIGURATION

LANGUAGE

PROXY

FONTS

ACCESS TIME

SIM CARD

BATTERY USAGE

SETTINGS

InMobile

InMobile®

Deep mobile device intelligence to layer into risk assessment and fraud prevention strategies and security mechanisms to protect your customers

PERMANENT DEVICE IDENTIFICATION

DEVICE INTEGRITY SCREENING

DEVICE ANALYSIS & SCORING

CYBERSECURITY MECHANISMS

- ✓ Deployed as an SDK into your business mobile app
- ✓ On-premise or cloud deployment
- ✓ Enables binding of device and user and establishes the device as trusted 2nd factor of authentication proving “something you have”
- ✓ Detects risky vs. non-risky devices

InPermID ®

Persistent device prints may suffer change when subjected to factory reset or operating system changes, making them an unreliable factor of authentication

InAuth collects unique attributes from the mobile device to create a unique and permanent device print, **InPermID**

The only **unique** and **permanent** mobile device ID available

Detect legitimate & repeat devices for frictionless authentication and transactions

Cannot be spoofed, altered, replayed

Prevent repeat attacks from fraudsters with negative device history

Device Integrity Screening

For presentation purposes only

MALWARE AND CRIMEWARE DETECTION

The InAuth Malware research team utilizes over 50 industry leading malware feeds to scan for malware threats. Malware signature lists are updated as threats evolve and require no download by the customer or \marketplace push to the app store.

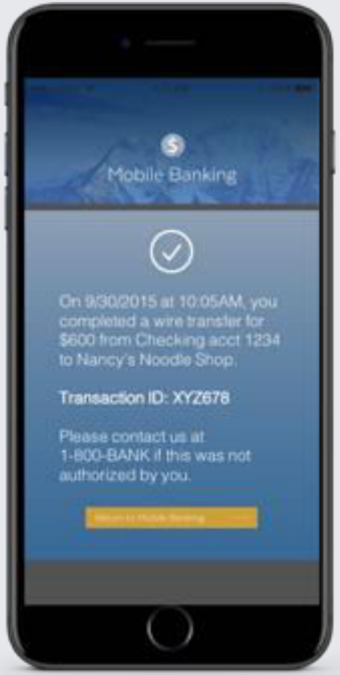
CLOAKED ROOT / HIDDEN JAILBREAK DETECTION

Identifies devices that have been rooted or jailbroken, but also protects against increasingly more complicated methods used by fraudsters, such as Cloaked Root and Hidden Jailbreak, where a fraudster has rooted and jailbroken their device and is attempting to mask its status.

APPLICATION VALIDATION

Confirms the integrity of your business’s mobile application by confirming the app has not been tampered with or modified through malicious activity.

Cybersecurity Mechanisms



On 9/30/2015 at 10:05AM, you completed a wire transfer for $600 from Checking acct 1234 to Nancy's Noodle Shop.

Transaction ID: XYZ678

Please contact us at 1-800-BANK if this was not authorized by you.

For presentation purposes only. UI and message to be generated by client.

POLICY-BASED WHITE BOX

Secure & encrypted storage of sensitive data within your business's mobile app. Prevents fraudulent activity based on device integrity and is only accessible by your business's app. Allows access to White Box even in offline mode. In compliance with GDPR, White Box provides secure and encrypted storage of all PII data, which can be destroyed if required.

SECURE MESSAGING

Securely packages contextual messages for delivery to a device associated with an InPermID. Reduces reliance on costly, ineffective, and insecure 3rd party message providers.

CERTIFICATE PINNING

Avoids traffic interception between a legitimate mobile app and server that is utilizing rogue or fraudulent security certificates. InAuth will pin and only trust the correct certificate issued exclusively by our client. The certificate is securely stored within the InAuth Soft Secure Element, the encrypted, secure storage component of our InMobile SDK, protecting it from attack.

InBrowser

InBrowser®

Best-in-class technology to authenticate any web-connected device with a browser through next-generation fingerprinting

- ✓ Deployed via JavaScript
- ✓ Includes mobile browsers, desktop/laptops, smart TVs, gaming consoles, etc.
- ✓ On-premise or cloud deployment
- ✓ Detects risky vs. non-risky devices
- ✓ Enables binding of device and user and establishes the device as trusted 2nd factor of authentication proving “something you have

NEXT-GENERATION BROWSER FINGERPRINT

DEVICE ANALYSIS & SCORING

BROWSER AGNOSTIC

InAuth leverages high-tech technology and device-specific browser identification to produce a strong, persistent browser fingerprint, **InBrowserID^{TM}**

Uniqueness and longevity are key elements for device fingerprint effectiveness as a factor of authentication

- Industry-leading print stability and uniqueness, minimizing collision rates and maximizing fingerprint longevity
- Reduced false positives for trusted devices
- InBrowserID’s are returned within milliseconds and will always be returned by InAuth - even if JavaScript or Flash is disabled
- Spoof detection automatically detects fabricated or spoofed fingerprints

InRisk

InRisk®

Analyzing **device intelligence** to understand trustworthiness

Is this device trying to mask its location with a proxy or VPN or is it using spoofing tools?

What is the reputation of this device at other companies?

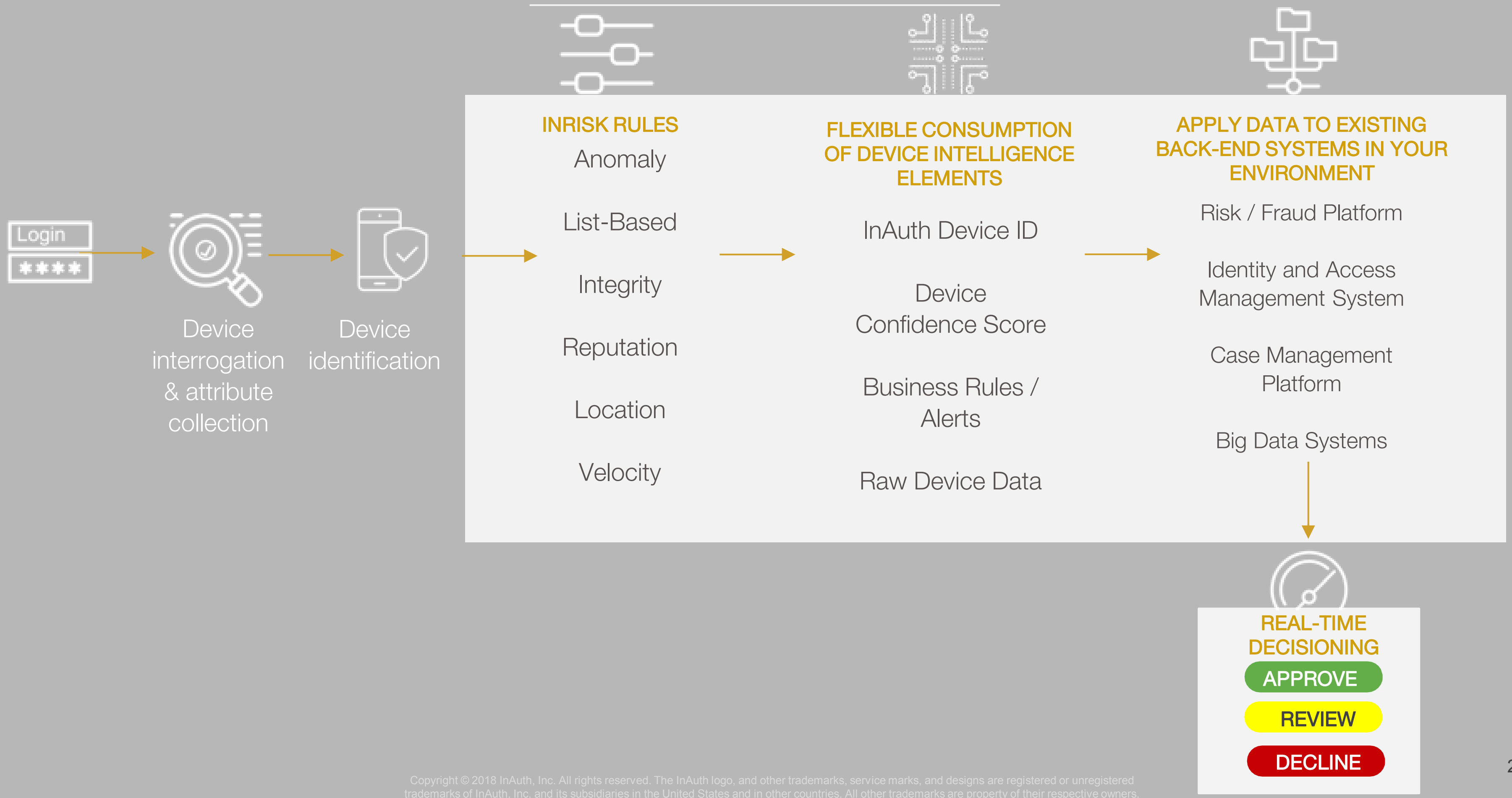
Has the device conducted multiple transactions over a short period of time or tried to access other accounts

Is this the device the customer typically uses?

Has the device been stationary or full battery charge for a long period of time?

Are the location attributes consistent?

InRisk® in Action



Device interrogation & attribute collection

Device identification

INRISK RULES

- Anomaly
- List-Based
- Integrity
- Reputation
- Location
- Velocity

FLEXIBLE CONSUMPTION OF DEVICE INTELLIGENCE ELEMENTS

- InAuth Device ID
- Device Confidence Score
- Business Rules / Alerts
- Raw Device Data

APPLY DATA TO EXISTING BACK-END SYSTEMS IN YOUR ENVIRONMENT

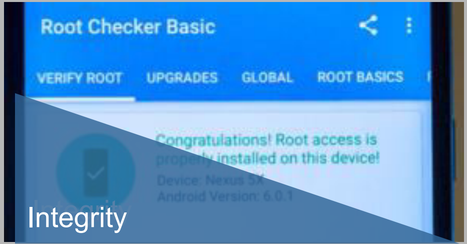
- Risk / Fraud Platform
- Identity and Access Management System
- Case Management Platform
- Big Data Systems

REAL-TIME DECISIONING

- APPROVE
- REVIEW
- DECLINE

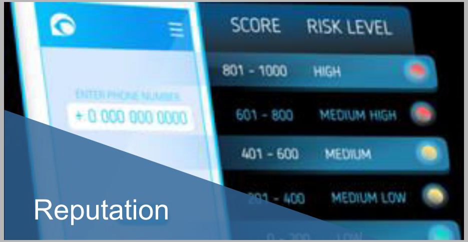
InRisk® InMobile Business Rules

- LOCATION INCONSISTENCY
- BATTERY PLUGGED IN
- PHONE OR TABLET DEVICE NOT MOBILE
- ANDROID: UNKNOWN SOURCES ENABLED
- RISKY LANGUAGE
- HIGH RISK FONT
- UNUSUAL CUSTOMER ACCESS TIME
- SIM CARD DELTA
- MAKE MODEL CONSISTENCY
- OS VERSION CONSISTENCY
- EMULATOR DETECTION
- SPOOF DETECTION



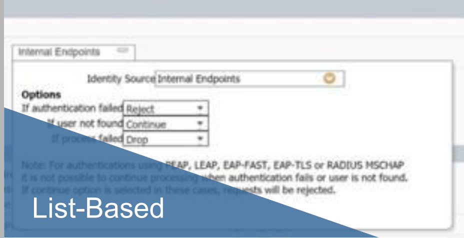
Congratulations! Root access is properly installed on this device!
Device: Nexus 5X
Android Version: 6.0.1

- CLOAKED ROOT DETECTION
- CRIMEWARE/MALWARE INSTALLED
- MALWARE DETECTION AND CATEGORY POPULATON
- DEVICE NAME CHANGE



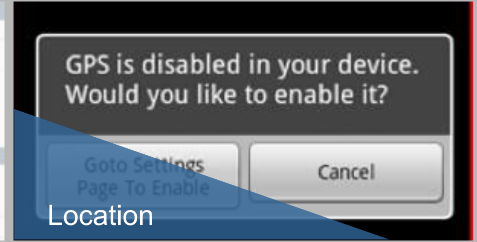
SCORE	RISK LEVEL
801 - 1000	HIGH
601 - 800	MEDIUM HIGH
401 - 600	MEDIUM
201 - 400	MEDIUM LOW
0 - 200	LOW

- GLOBAL DEVICE REPUTATION NETWORK



Identity Source Internal Endpoints
Options
If authentication failed Reject
If user not found Continue
If process failed Drop
Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

- APPLICATION NAME NEGATIVE LIST
- DEVICE NEGATIVE LIST
- COUNTRY LOCATION POSITIIVE LIST



GPS is disabled in your device. Would you like to enable it?

- GPS DISABLED
- GEO-RADIUS
- NEW LOCATION
- NON-US LOCATION

InAuthenticate

InAuthenticate®

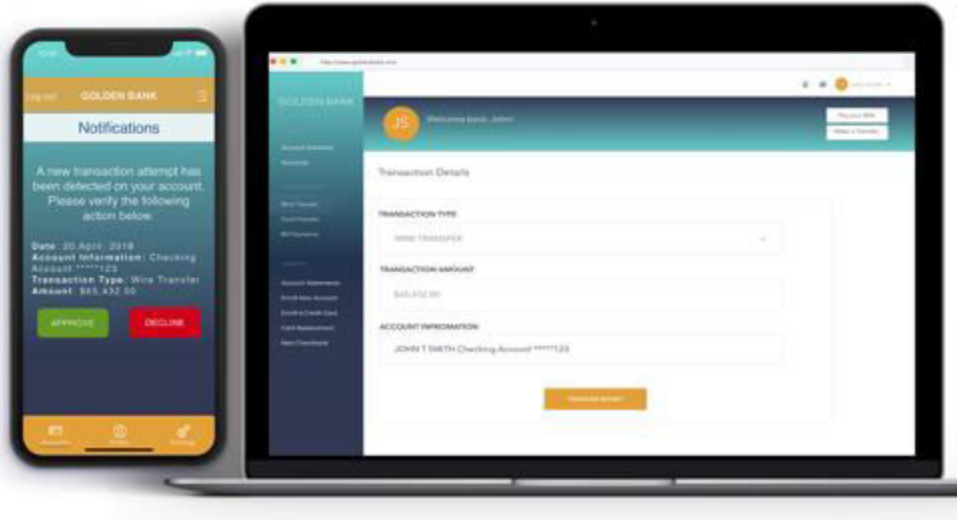
Current out-of-band channels to verify authenticity, such as SMS, email, or call centers, are insecure and easily compromised by fraudsters through malware, man-in-the-middle interception, and other techniques. They also produce friction for consumers, resulting in abandoned transactions and increased operational costs.

Incorporated as an SDK within your business's mobile app, **InAuthenticate** goes into action when strong customer authentication is needed for:

✓ Login
✓ Transfers
✓ Payment transactions
✓ Account changes
✓ Dual approvals
✓ Customer acknowledgements or consent

Secure Two-Factor Authentication Solution

InAuthenticate enables your organization to send a secure authentication message to your customer's registered mobile device. The customer simply opens your mobile app to receive an authentication message and responds accordingly by confirming or denying the transaction.



A new transaction attempt has been detected on your account. Please verify the following action below.

Date: 20 April, 2018
Account Information: Checking Account ******123
Transaction Type: Wire Transfer
Amount: $65,432.00

Transaction Details

TRANSACTION TYPE: WIRE TRANSFER
TRANSACTION AMOUNT: $65,432.00
ACCOUNT INFORMATION: JOHN T SMITH Checking Account *****123

For presentation purposes only. UI and message created by client.

InAuthenticate® Technology

Trusted Path

Trusted Path is our secure channel of communication, providing an encrypted pathway between the InAuthenticate SDK and InAuth Server to send sensitive messages. Trusted Path leverages banking-grade cryptographic algorithms to provide strong protection.

InPermID

InAuthenticate messages sent through Trusted Path can only be read by devices identified with an InPermID, our permanent device identifier for mobile apps.

Device Integrity Screening

InAuthenticate utilizes cybersecurity mechanisms in order to identify risky device behaviors including malware detection, geolocation inconsistency cross-checks, anti-tamper verification, and cloaked root / hidden jailbreak detection.

STRONG CUSTOMER AUTHENTICATION

Utilizes a unique and permanent device ID in order to identify and recognize returning devices, allowing you to authenticate users with confidence

SECURE MESSAGE DELIVERY

Protected by InAuth's Trusted Path, our encrypted communication channel, for secure server-to-client message delivery

CONTEXTUAL MESSAGING

InAuthenticate messages are contextual, allowing your customers to easily understand the authentication request and respond by confirming or denying the transaction

REDUCED FRICTION

Reduced need for your customers to install additional downloads or clunky hardware, keeping your customers in your business's footprint and allowing them to complete transactions with greater ease

FRAUD PREVENTION

Advanced device screening to detect compromise and prevent fraud

REDUCED OPERATIONAL COSTS

Reduced reliance on email or SMS passcodes and call center authentication

03

Why InAuth

What Makes **InAuth** Unique

- Breadth of Products & Services
- Deep Device Intelligence & Fraud Expertise
- Next-Generation Device ID
- Marquee Clients & Partners from across industries
- Flexible Deployment On Premise or Hosted
- Real-time Responsiveness & Platform Stability

What Makes InAuth Unique

JPMorgan

AMERICAN EXPRESS

WELLS FARGO

Bank of America

Capital One

TÜRKİYE İŞ BANKASI

TESCO Bank

KBC

ING

Virgin money

AIB Allied Irish Bank

Nationwide Building Society

NICE · ACTIMIZE

Accertify an American Express company

CyberSource® the power of payment

FEATURE SPACE

COSTCO WHOLESALE

WESTERN UNION moving money for better

Expedia

BEST BUY

priceline.com

UBER

Sunil Gossain
InAuth SVP
Sunil.gossain@inauth.com
+44(0)7850 796319

InAuth

Digital Intelligence Experts