IPification

M-Identity Remastered

Passwordless Tomorrow Begins Today. No credentials, tokens, SMS OTPs, header enrichment, or face scans. A single tap with unparalleled security.

www.ipification.com

IPification

- IPification is the advanced Mobile Identity brand within Benefit Vantage Limited, a Hong Kong-based company also running initiatives in Cyber Security solutions, Data Protection & Backup and Mobile Content Distribution
- Staff in 9 locations – USA, Hong Kong, Belgrade, Vietnam, Schaffhausen (CH), Sarajevo, UK, Brazil, India
- IPification solution offers IP-based Operator Discovery, Seamless Authentication, Device Verification, SIM and Device Swap and Location/Proximity solutions all based on a simple, fast and low-cost deployment model
- Live implementations with 18 mobile operators on 4 continents; 50+ mobile operators currently in implementation phase
- www.ipification.com

A GLOBAL VIEW

GLOBAL CYBERCRIME IN NUMBERS

Mobile Attacks Outpace Desktop for the First Time

19B Transactions Processed

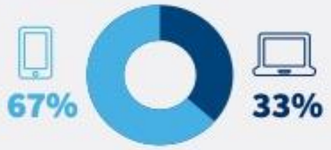
401M Attack Volume

171% Growth in Mobile App Attack Rate YOY

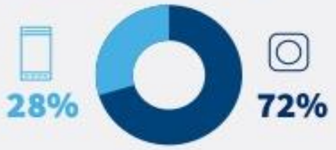
Attack rate is based on percentage of transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically and in near real time depending on individual customer use cases.

TRANSACTIONS PROCESSED: 19B

Transactions Split by Mobile / Desktop



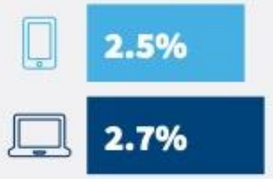
Transactions Split by Mobile Browser / App



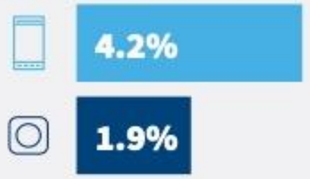
ATTACK TRENDS

Attack Volume | **401M** TOTAL | **264M** | **137M**

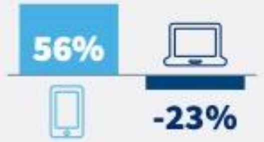
Attack Rates Mobile / Desktop



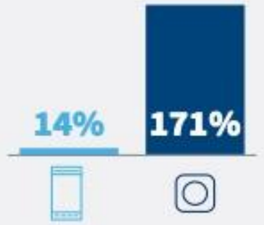
Attack Rates Mobile Browser / App



Attack Rate Growth YOY Mobile / Desktop



Attack Rate Growth YOY Browser / App



A GLOBAL VIEW

ATTACK VOLUME GROWS IN NEW ACCOUNT ORIGINATIONS AND PAYMENTS

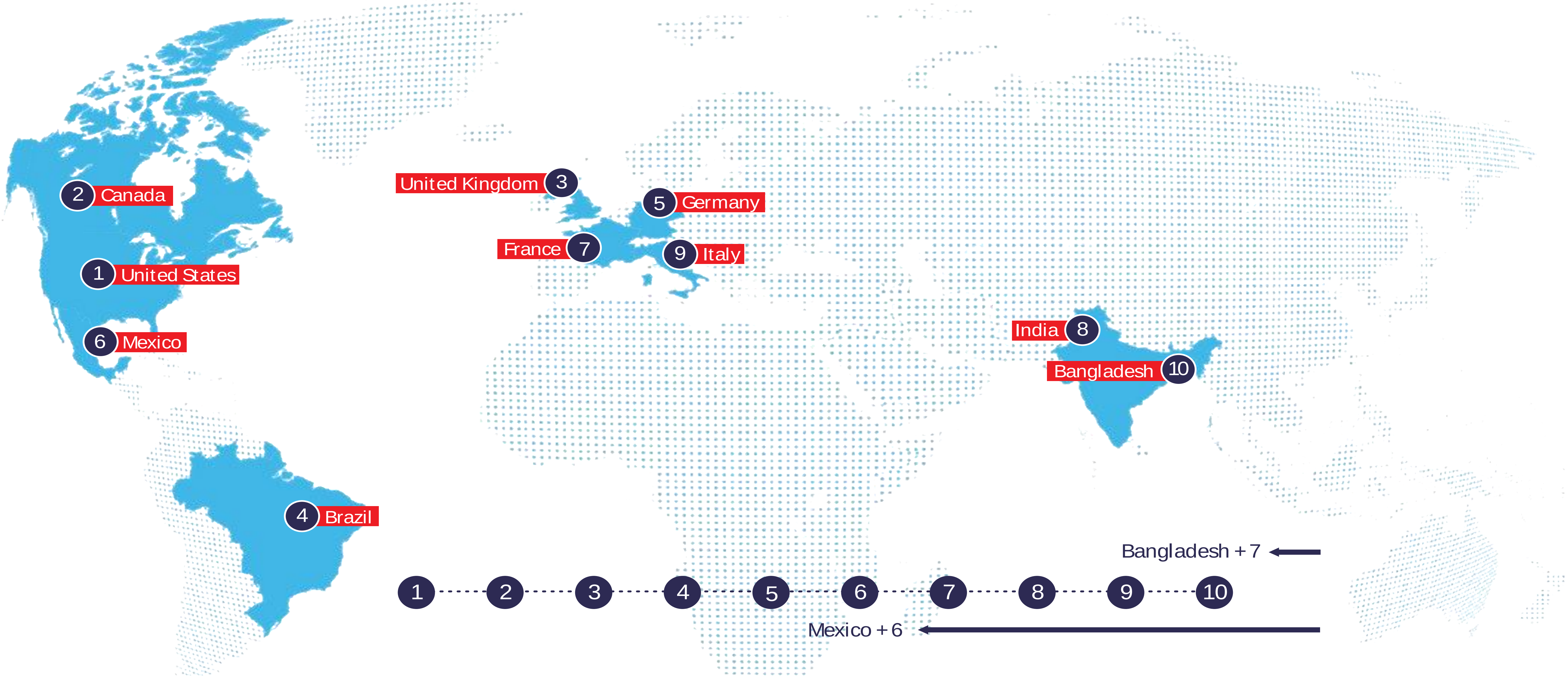
	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK VOLUME	132M	110M	105M
ATTACK RATE	17.0%	1.0%	4.1%
ATTACK RATE GROWTH / DECLINE YOY	+293% Growth in Attack Volume +39% Growth in Attack Rate	-13% Decline in Attack Volume -38% Decline in Attack Rate	+58% Growth in Attack Volume -7% Decline in Attack Rate
	New account creations are most at risk during this period, as a result of a large global bot attack targeting new mobile app registrations.	Logins are the safest transactions as a proportion of overall transaction volume; repeat transactions help businesses to build trust levels of good, returning users.	The growth in payment attacks is slightly less than the growth in payment transaction volume, indicating a stable risk environment despite a moderate attack rate.

** Attack volume and attack rate are calculated using a subset of the total transaction volume, where outliers, and attacks on some transaction types such as change of details and internal transfers are removed.*

A GLOBAL VIEW

SPREAD OF TOP ATTACKERS CONFIRMS CYBERCRIME IS A TRULY GLOBAL INDUSTRY

All Key Regions Represented in the Top Attackers List



A REGIONAL VIEW

APAC EXPERIENCES STRONG BOT ACTIVITY

Automated Attacks Target Financial Services New Account Creations

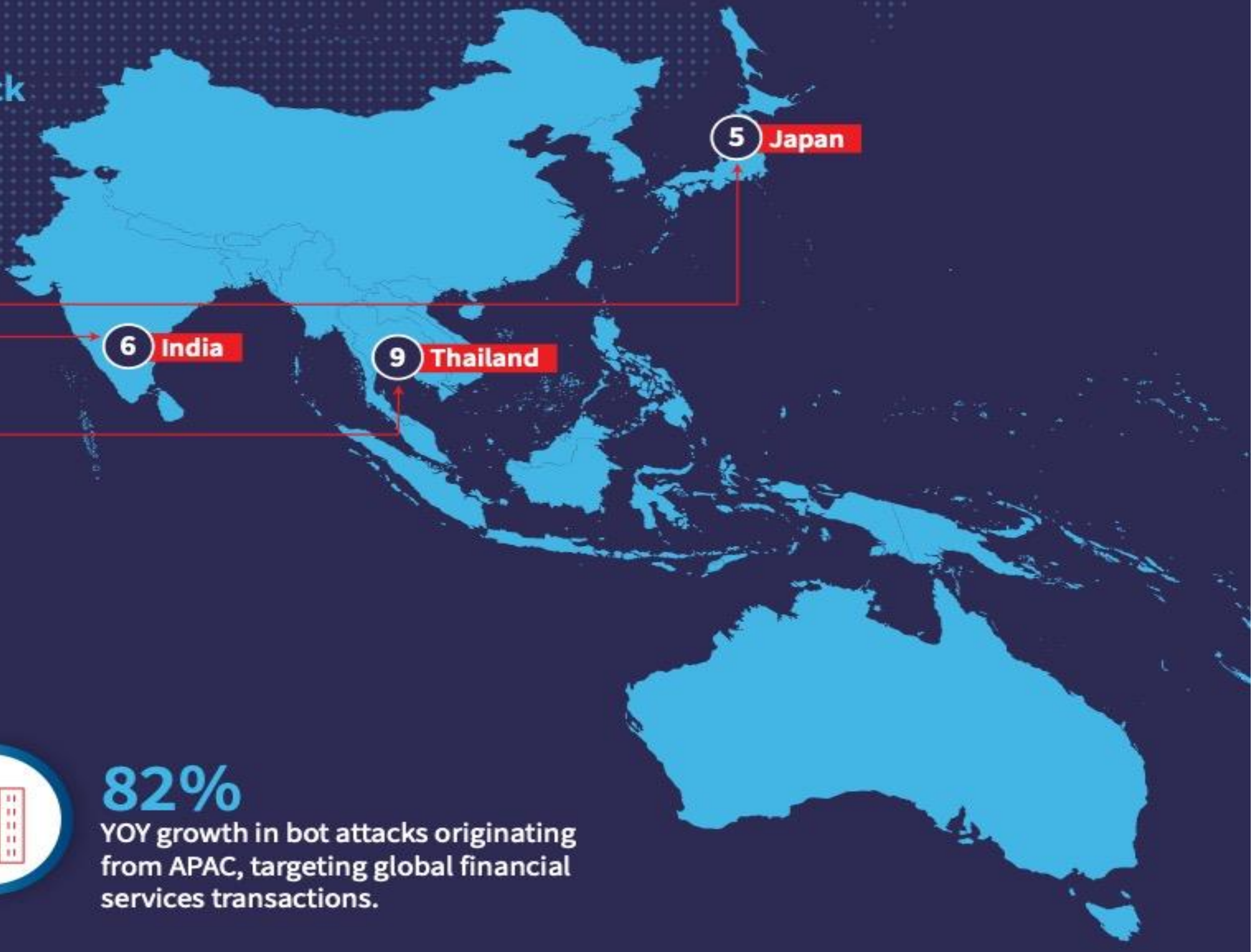
While some of this bot traffic comes from “good” bots, namely aggregators accessing financial services organizations, a high percentage of attacks are maliciously targeting logins and new account creations using stolen or spoofed identity credentials.

Bots originate from the most highly developed of APAC countries, through to emerging and growth economies. This shows the widespread dissemination and use of breached identity data.

Bot traffic in the APAC region is predominantly targeting financial services institutions, specifically new account creation processes.

Top 10 Bot Attack Originators

1. U.S.
2. UK
3. Canada
4. Germany
5. Japan
6. India
7. Brazil
8. France
9. Thailand
10. Russia



82%
YOY growth in bot attacks originating from APAC, targeting global financial services transactions.

A REGIONAL VIEW

APAC AND MIDDLE EAST-FOCUSED FRAUD NETWORK

Cross-Over Between Financial Services and E-Commerce Organizations

Anatomy of Fraud Network

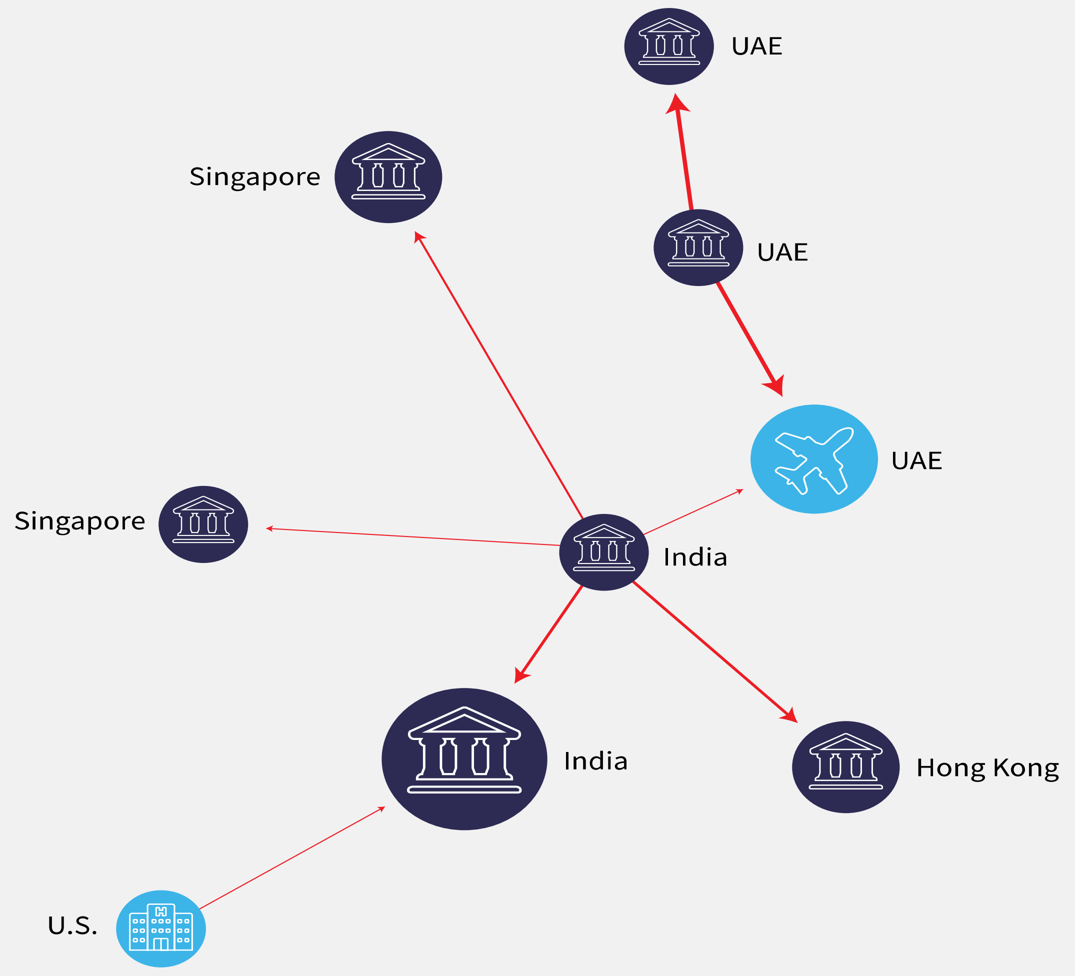
200
Devices associated with fraud, cross over with more than one organization.

900
Cross-organizational events are login transactions.

150
Cross-organizational events are payment transactions.

$11M+
Exposure to fraud at original organization.

$350k
Exposure to fraud at cross-over organizations in one-month period.



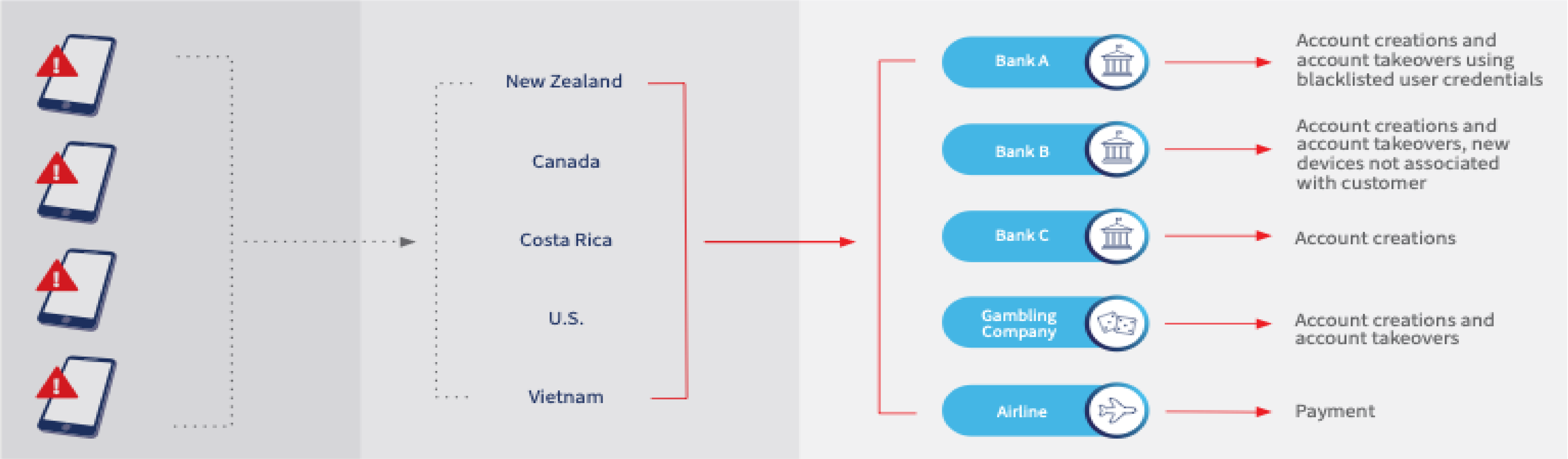
FINANCIAL SERVICES: BANK

E-COMMERCE: HEALTHCARE TRAVEL

A larger circle denotes a larger organization by transaction volume. A thicker line denotes a higher volume of fraud.
Less than 10 device overlaps between companies have been removed.

A BUSINESS VIEW:
BANKING

TRACKING FRAUDULENT ACTIVITY ACROSS THE NETWORK



New Zealand

Canada

Costa Rica

U.S.

Vietnam

Bank A — Account creations and account takeovers using blacklisted user credentials

Bank B — Account creations and account takeovers, new devices not associated with customer

Bank C — Account creations

Gambling Company — Account creations and account takeovers

Airline — Payment

1 Linked Devices

4 Devices linked to 1 IP address and 52 different

2 Multiple Locations

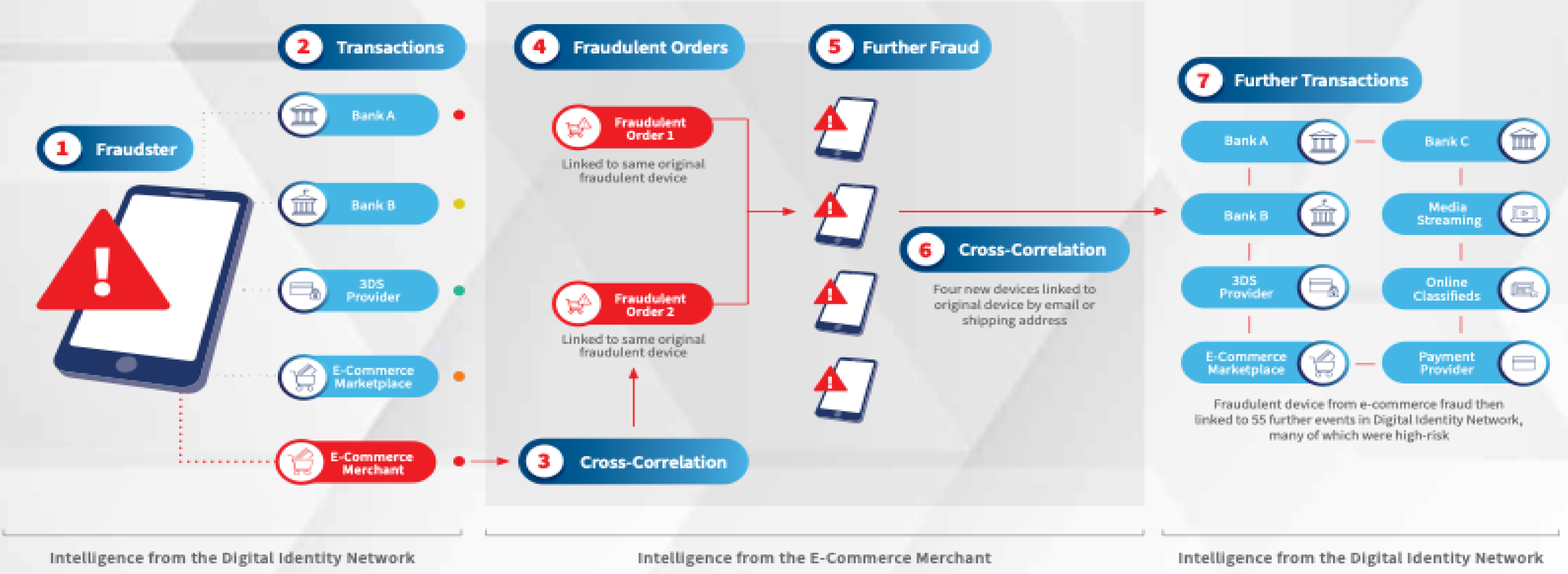
Devices appear to come from 5 different locations across 3 regions

3 Events in Digital Identity Network

81 events seen at 5 different organizations in the Digital Identity Network

COLLABORATION WITH E-COMMERCE MERCHANT REVEALS COMPLEX, NETWORKED FRAUD

● LOW-RISK ● MEDIUM-RISK ● HIGH-RISK ● REJECTED



1 Fraudster

2 Transactions

Bank A

Bank B

3DS Provider

E-Commerce Marketplace

E-Commerce Merchant

3 Cross-Correlation

4 Fraudulent Orders

Fraudulent Order 1

Linked to same original fraudulent device

Fraudulent Order 2

Linked to same original fraudulent device

5 Further Fraud

6 Cross-Correlation

Four new devices linked to original device by email or shipping address

7 Further Transactions

Bank A

Bank C

Bank B

Media Streaming

3DS Provider

Online Classifieds

E-Commerce Marketplace

Payment Provider

Fraudulent device from e-commerce fraud then linked to 55 further events in Digital Identity Network, many of which were high-risk

Intelligence from the Digital Identity Network

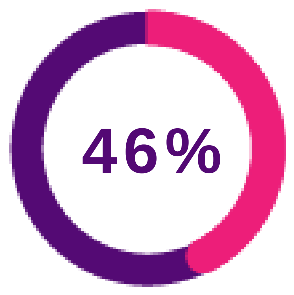
Intelligence from the E-Commerce Merchant

Intelligence from the Digital Identity Network

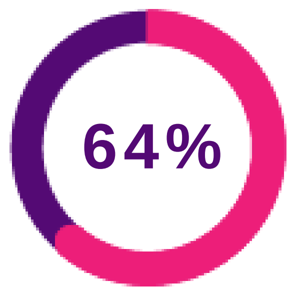
Financial Frauds in Asia-Pacific

Risky Mobile Money & Mobile Banking

Most users get compromised via Mobile Phone Services, SMS and Phone Call following up with the social media and email frauds.



The Unreported Frauds



No Money-Back Victims

Commonly affected services

MOBILE MONEY

MOBILE BANKING

ONLINE BANKING

BANK CHEQUE

92% Move Bank

Most users would move bank or financial service provider for an organisation that offers a more secure service to protectagains fraud.

83% Leave Bank

Africans would leave their bank of financial service provider if they didn’t do enough to protect against financial fraud.

80% Pay Fee

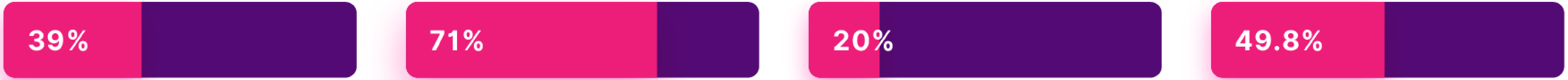
80% said they’d be prepared to pay a small fee to prevent fraud on financial transactions.

Financial Frauds in Asia-Pacific

Protecting Consumer Trust

Experian’s Digital Consumer Insights 2018 shows that Asian mobile payment providers enjoy the trust of a large consumer base. However, recent studies show a 30% rise in the number of fraud incidents.

Mobile payment landscape



Asia Pacific’s adults are unbanked

Consumers prefer online purchases

Mobile payments are fraud victims

Consumers have experienced fraud

Fraud type Examples

Fraud type Examples

Theft of mobile money via Mobile Malware.

Subscription Fraud against Mobile Money Service.

Account hijack via Sim Swap and MSISDN change.

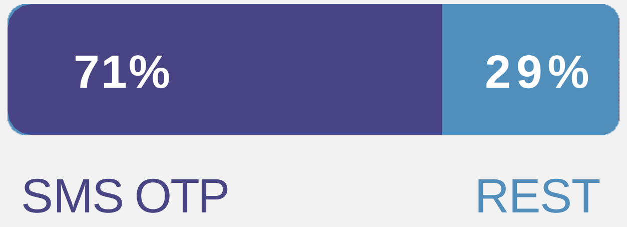
Authorization SMS spoofing.

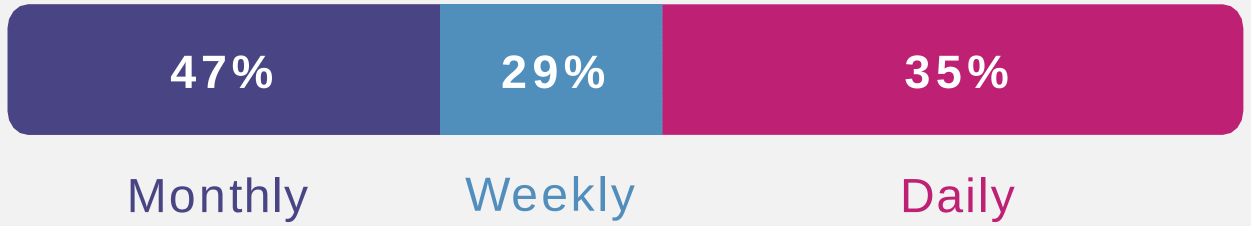
SIM swap fraud is one of the most prolific forms of financial service fraud

9O%	African banking leaders identify SIM swap as an issue for their organisations
57%	Consumers have been victims of SMS-phishing
74%	Financial institutions in Africa use one-time-password(OTP) via SMS

Statistical overview

Financial transaction services done over the SMS OTP





A review on Authentication Methods

Deprecated Mobile Authentication Options

Users are facing many difficulties in mobile authentication space today, mostly related to security vulnerabilities (plain/ insecure protocols - SS7 breaches, HTTP sniffing), privacy leaking (sharing sensitive data without users' awareness - MSISDN) and bad user experience (multiple user interactions during SMS OTP)

Unfriendly 😐
SMS One Time Pin

Already deprecated in many countries

SS7 insecure protocol

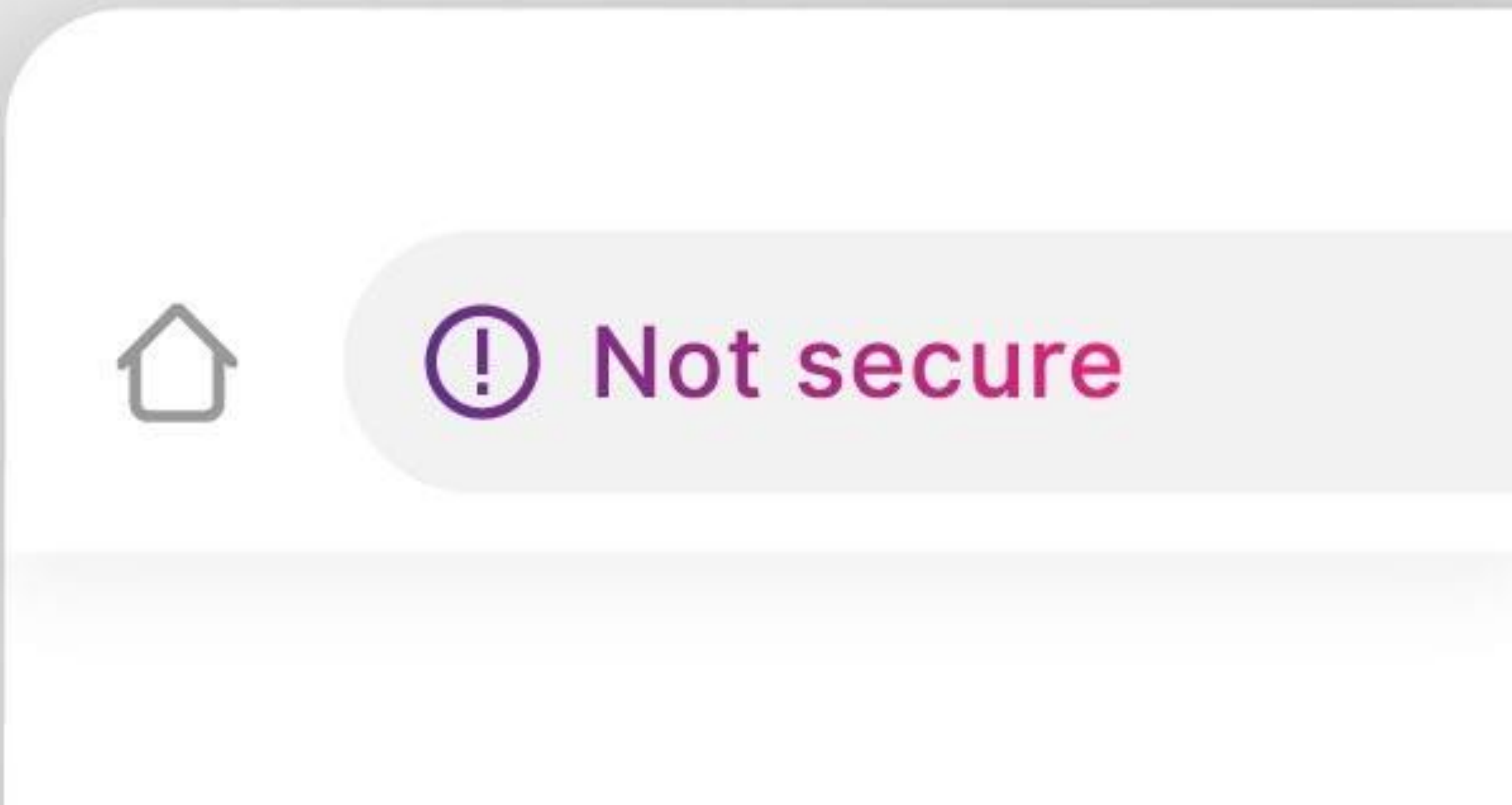
Bad User Experience = bad conversion rates

Insecure (!)
Header Enrichment

Works only over the HTTP.

Apple will require HTTPS for all its iOSApps.

"Not Secure" all browsers warning.



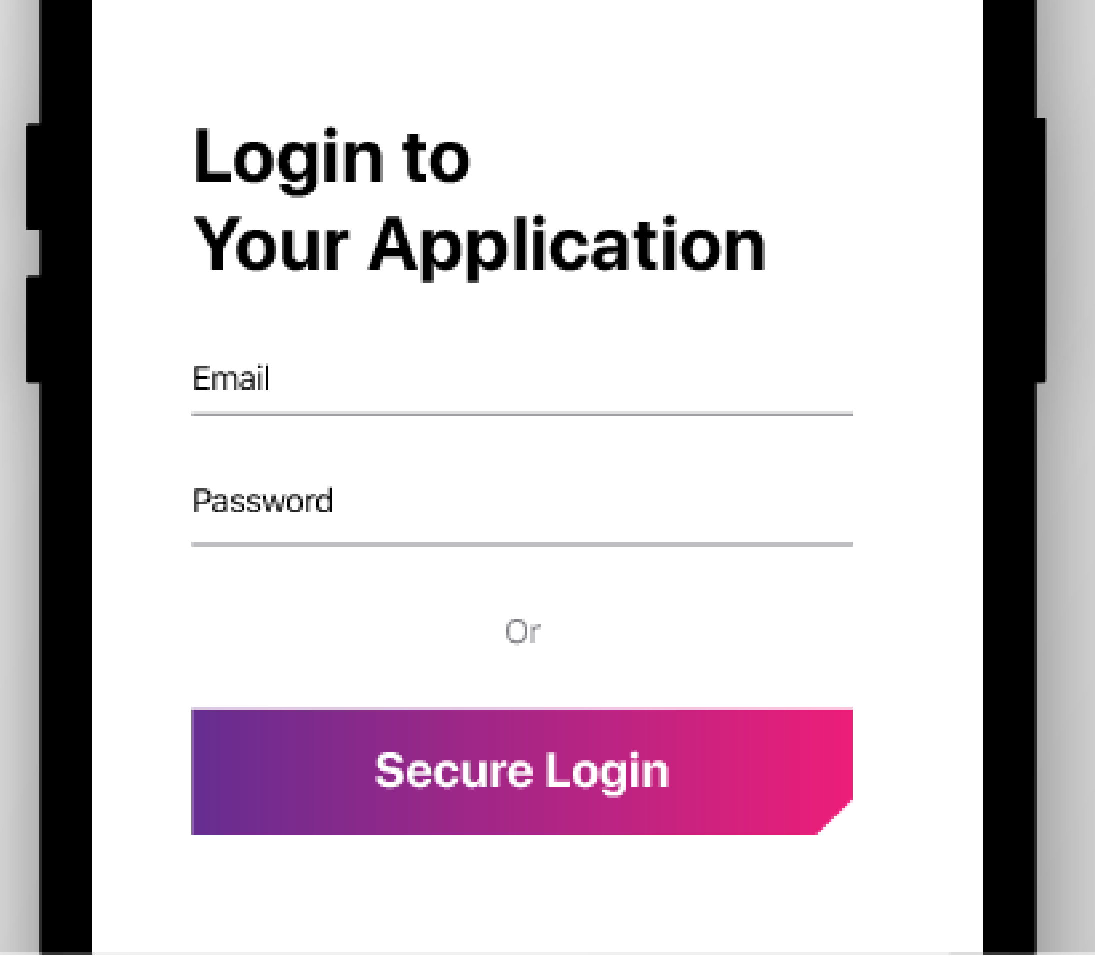
The Future of Mobile Authentication with IPification

Where Simplicity & Safety Meet Authentication

Highly secure, credential-less, network-based authentication solution for smooth UX on user mobile and IoT devices.

Auth Revolution

Designed to facilitate instant user access infused with bank grade security IPification leverages authentication possibilities outside traditional SMS, header enrichment and USSD.



Propreietary and patented
HH(1248463)
US(15928348)
UH(1803719.2)

Security

Secure protocols for user’s identity confirmation based on mobile network data only

Privacy

Not taking any application/device information, no way for sensitive information leak

Access

Zero-click compatible and Mobile Connect compliant authentication solution

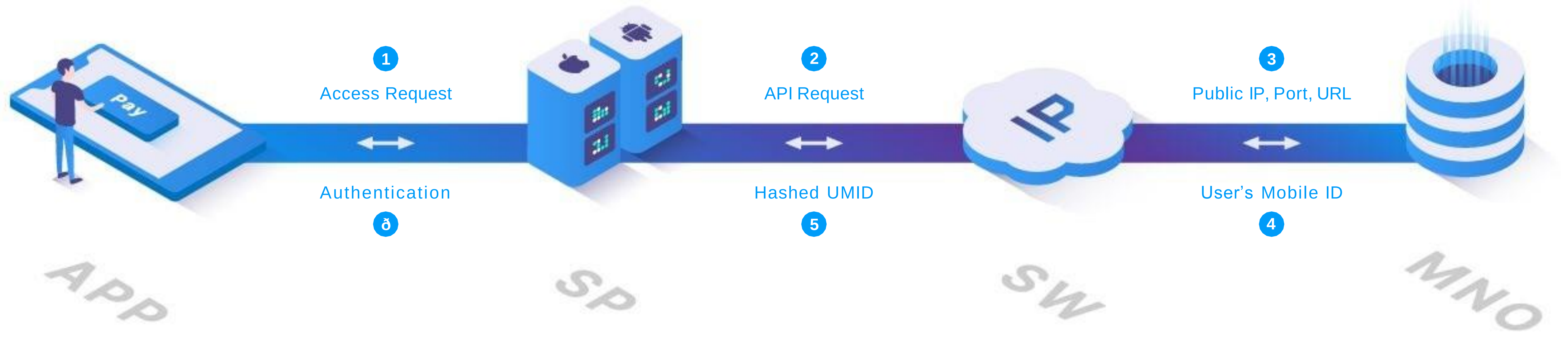
GSMA COMPLIANT

GSMA’s identity standard allows consumers across the globe to access their accounts via a single login, without the need for passwords and usernames. GSMA has endorsed IPification’s technology as the authentication standard for their identity programme

How it works

Unlocking the True Potential of M-Identity

By delivering Authentication as a Service (AaaS technology) to Telecoms via the **GMID” Box**, IPification reduces business costs, opens new revenue streams and enhances users security. Service providers and their users benefit from instant account access with improved privacy.



The IPification ‘Golden Triangle’

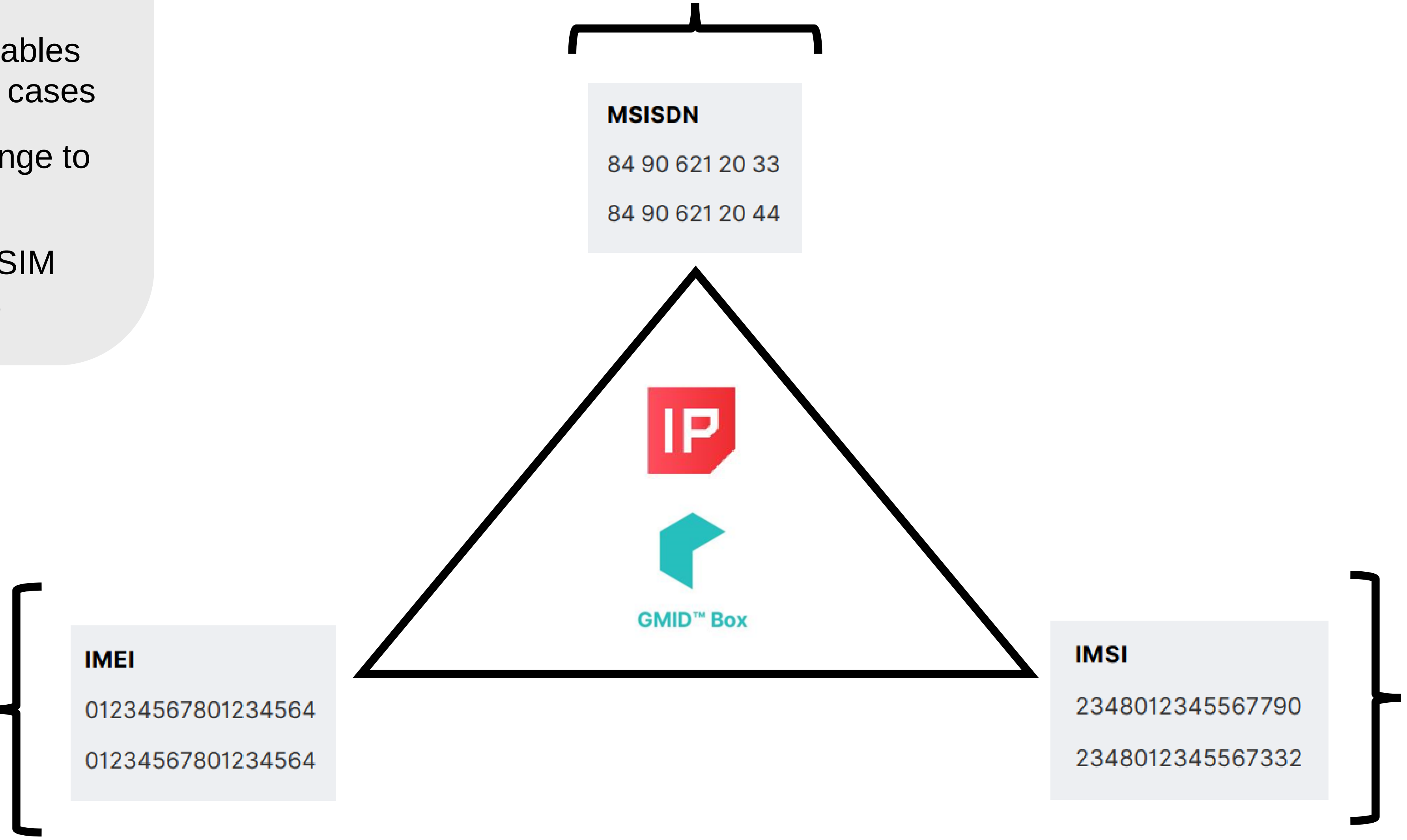
IPification GMiD Box:

- Generate unique hashed value for subscriber, device and SIM
- Persistent hash (no change) enables device and SIM verification use cases
- Change to ANY value flags change to subscriber status
- IMSI and IMEI changes create SIM Swap and Device Swap signals

MSISDN (*Mobile Station International Subscriber Directory Number*)

Subscriber Mobile Number

Unique globally with country prefix



MSISDN

84 90 621 20 33

84 90 621 20 44

IMEI

01234567801234564

01234567801234564

IMSI

2348012345567790

2348012345567332

IMEI (international mobile equipment identity)

Mobile Handset identification number

Unique globally

IMSI (international mobile subscriber identity)

SIM Card identification number

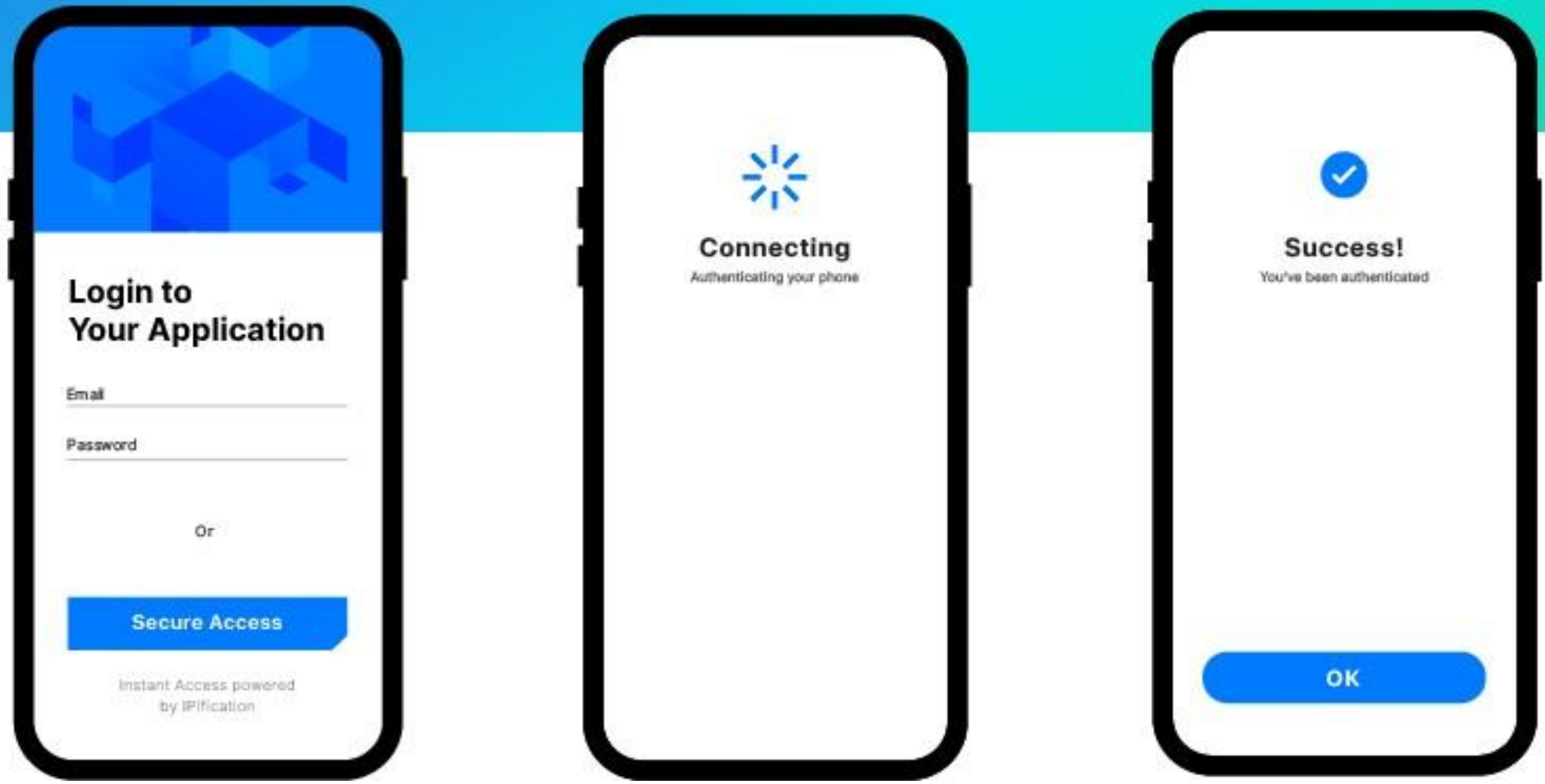
Unique globally

Auth UX

Zero-Click Compatible Access

Highly secure, relying on MNO network based information in real time

Web-based solution, not taking any information from the app/ device



Login to
Your Application

Email

Password

Or

Secure Access

Instant Access powered
by IPification

Connecting

Authenticating your phone

Success!

You've been authenticated

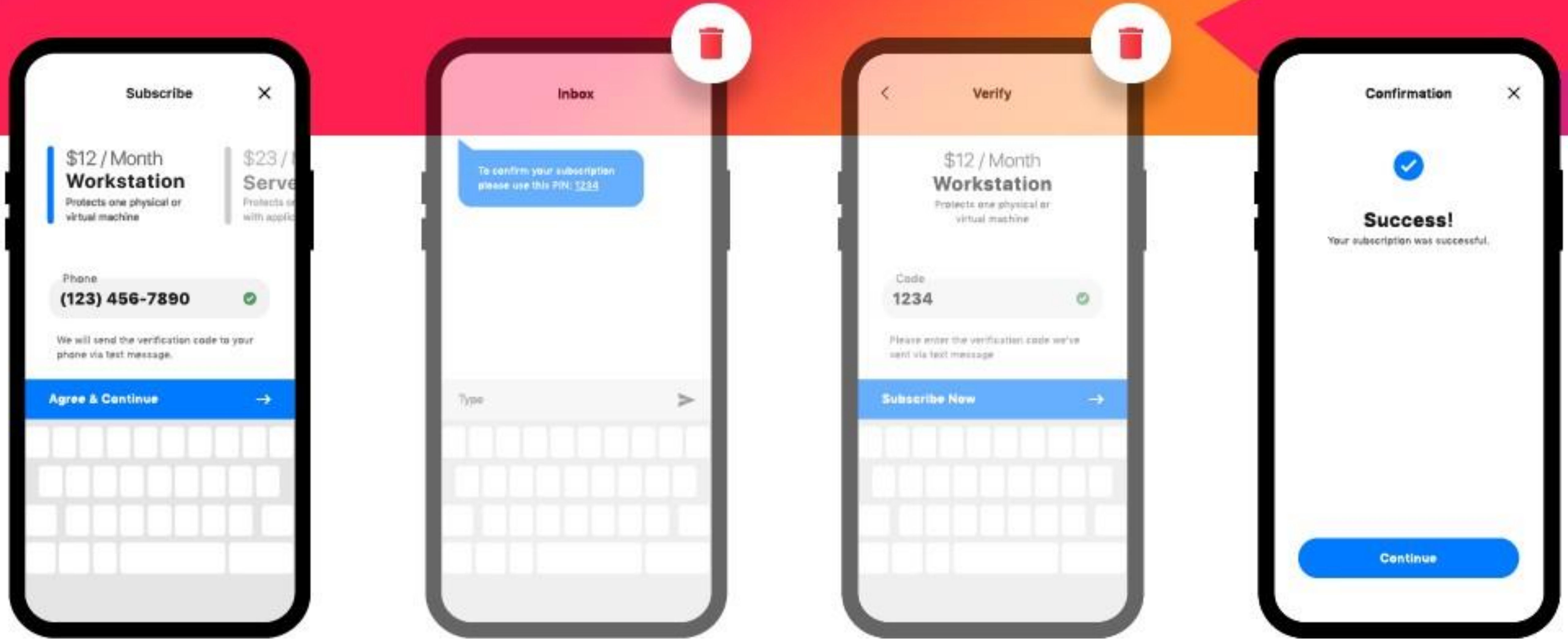
OK

Payments UX

The Convenient & Secure Revolution: IPification

Rapid evolution of authentication technology is making huge impact. Not only securing digital transactions but transforming them to even more convenient than ever.

IPification is designed to facilitate tap-and-go payments, infused with bank grade security.



Protects one physical or virtual machine

Phone: (123) 456-7890

We will send the verification code to your phone via text message.

To confirm your subscription please use this PIN: 1234

Protects one physical or virtual machine

Code: 1234

Please enter the verification code we've sent via text message

Your subscription was successful.

IPification eliminates excessive steps

Smart

Cambodia

Three.com.hk SmarTone

Hong Kong

TELKOMSEL

Indonesia

zain

Kuwait

CTM

Macau

T · ·

Montenegro

mts Telekom Srbija vip

Serbia

Dialog

Sri Lanka

bitel Telefonía móvil para todos

Peru

mobifone anytime anywhere

Vietnam

SK kt LG U+

South Korea

BSNL

Jio vodafone !dea airtel

India

IPification

Thank You

www.ipification.com

Harry Cheung, Founder & President

Serial entrepreneur with more than 20 years of experience in cybersecurity and data protection, Top 10 Business Entrepreneurs in China. – "Person of the Year in 2008"

Stefan Kostic, Chief Executive Officer

11years of experience in the FinTech & Telecom industries, ex C-level in Carrier Billing industry, Best Global Direct Carrier Billing (DCB) Aggregator in 2017 Award and Tier 1DCB vendor.

Aleksandar Brankovic, Chief Technology Officer

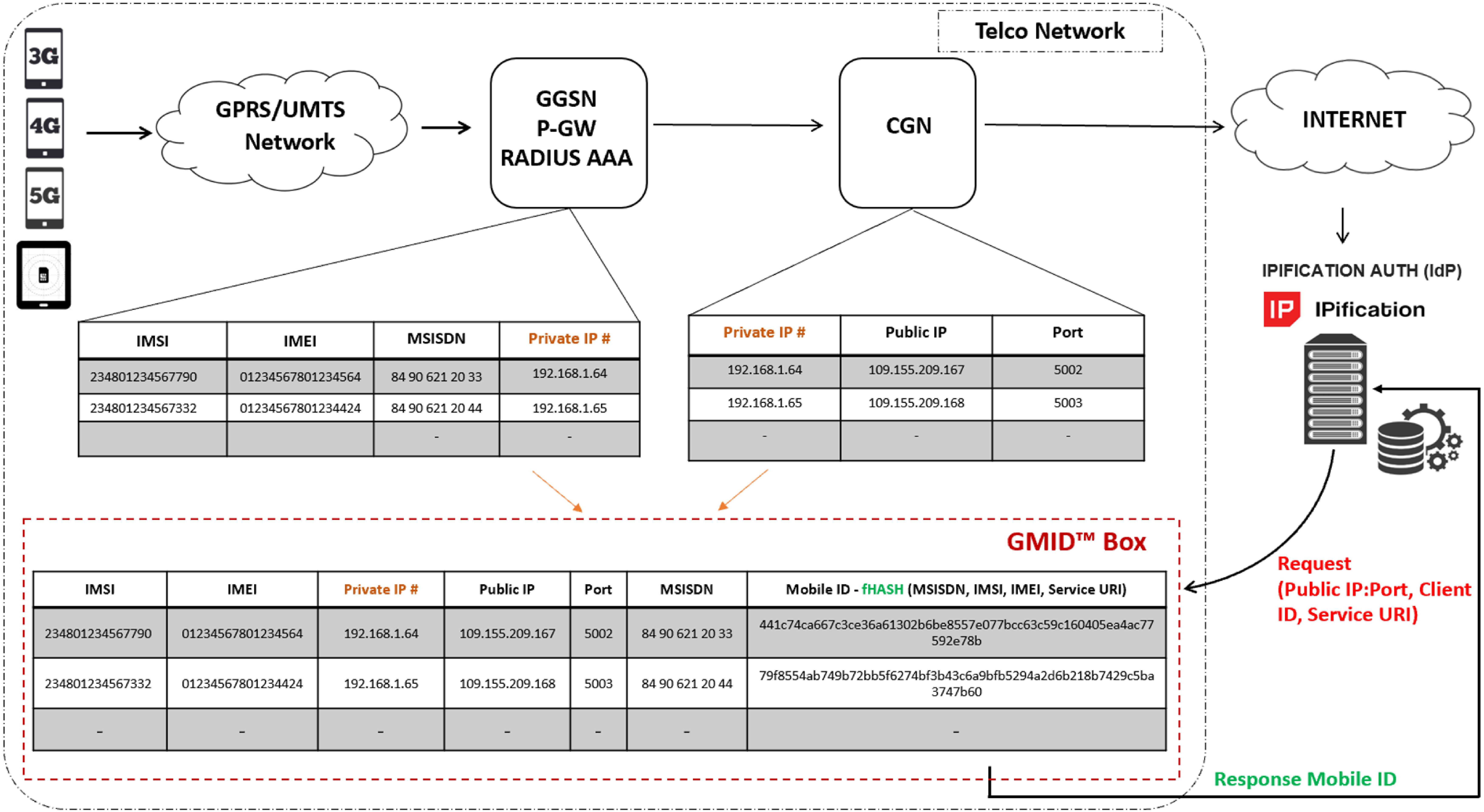
ICT professional with more than 15 years of extensive experience in anything technology-related.

Mark Harvey, Chief Revenue Officer

FinTech & Telecom industries business leader for more than 20 years, ex-GSMA Mobile Connect expert, top 100 influencers in Identity.

Jim Small, SVP Business Development

Over 25 years' experience driving delivery of technology-based new service in Telecom industry, ex Digital innovation leader in Orange UH and Orange Group Technocentre.



IMSI	IMEI	MSISDN	Private IP #
234801234567790	01234567801234564	84 90 621 20 33	192.168.1.64
234801234567332	01234567801234424	84 90 621 20 44	192.168.1.65
		-	-

Private IP #	Public IP	Port
192.168.1.64	109.155.209.167	5002
192.168.1.65	109.155.209.168	5003
-	-	-

IMSI	IMEI	Private IP #	Public IP	Port	MSISDN	Mobile ID - fHASH (MSISDN, IMSI, IMEI, Service URI)
234801234567790	01234567801234564	192.168.1.64	109.155.209.167	5002	84 90 621 20 33	441c74ca667c3ce36a61302b6be8557e077bcc63c59c160405ea4ac77592e78b
234801234567332	01234567801234424	192.168.1.65	109.155.209.168	5003	84 90 621 20 44	79f8554ab749b72bb5f6274bf3b43c6a9bfb5294a2d6b218b7429c5ba3747b60
-	-	-	-	-	-	-