

15 September 2026



GSMA™

The Network API Opportunity in Australia & NZ

Digital Trust & Growth Forum

Agenda

- **OGW Global Update**
- **Fusion**
- **Scam & Fraud Problem**
- **Commercial Opportunities**

OGW Global Update

GSMA Open Gateway website

GSMA Open Gateway

Universal mobile network open Application Programmable Interfaces (APIs) for developers.



MAP
API Deployments



API DOCUMENTATION
Usage guide and code snippets



USE CASE LIBRARY
API Use case examples



SANDBOX
Coming soon



MWC
MWC Shanghai 2025



SUPPORTERS
Operators and Channel Partners

API deployment map with certification status & links

GSMA™ Open Gateway

FILTERS

APPLIED (0)

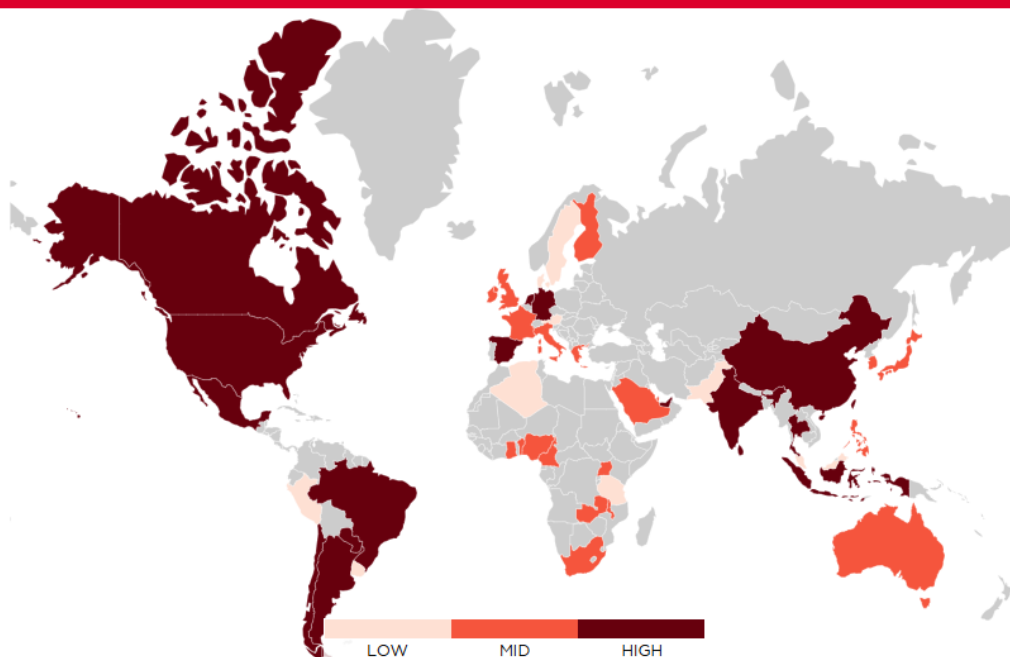
APIs (16)

REGIONS (8)

- ☐ Europe
- ☐ Sub-Saharan Africa
- ☐ North East Asia
- ☐ South East Asia
- ☐ Oceania
- ☐ Latin America
- ☐ North America
- ☐ Middle East and North Africa

MARKETS (47)

- ☐ Algeria
- ☐ Argentina
- ☐ Australia



API'S DEPLOYED (398)

Markets	Channel Partner	Provider	API Name	Version	Certified	Link
Spain	-	Orange	SIM Swap - Check	0.4.0	GSMA™ API Certified	Link
Spain	-	Orange	SIM Swap - Retrieve Date	0.4.0	GSMA™ API Certified	Link

☐ Country Grid

Export

Some key global OGW stats

Commitment

169 **89** operator groups and **80** Channel Partners supporting the Open Gateway MOU

303 operator networks represented

>80% of mobile connections represented

Assets

75 APIs published in
 **CAMARA**
THE TELCO GLOBAL API ALLIANCE

Technical

Standardization through certification
Certified APIs, Market View, Deployment Map

Commercial

Open Service Agreement, Channel Partner On-Boarding and E-W Federation Agreement Templates

Impact

347 commercial API launches

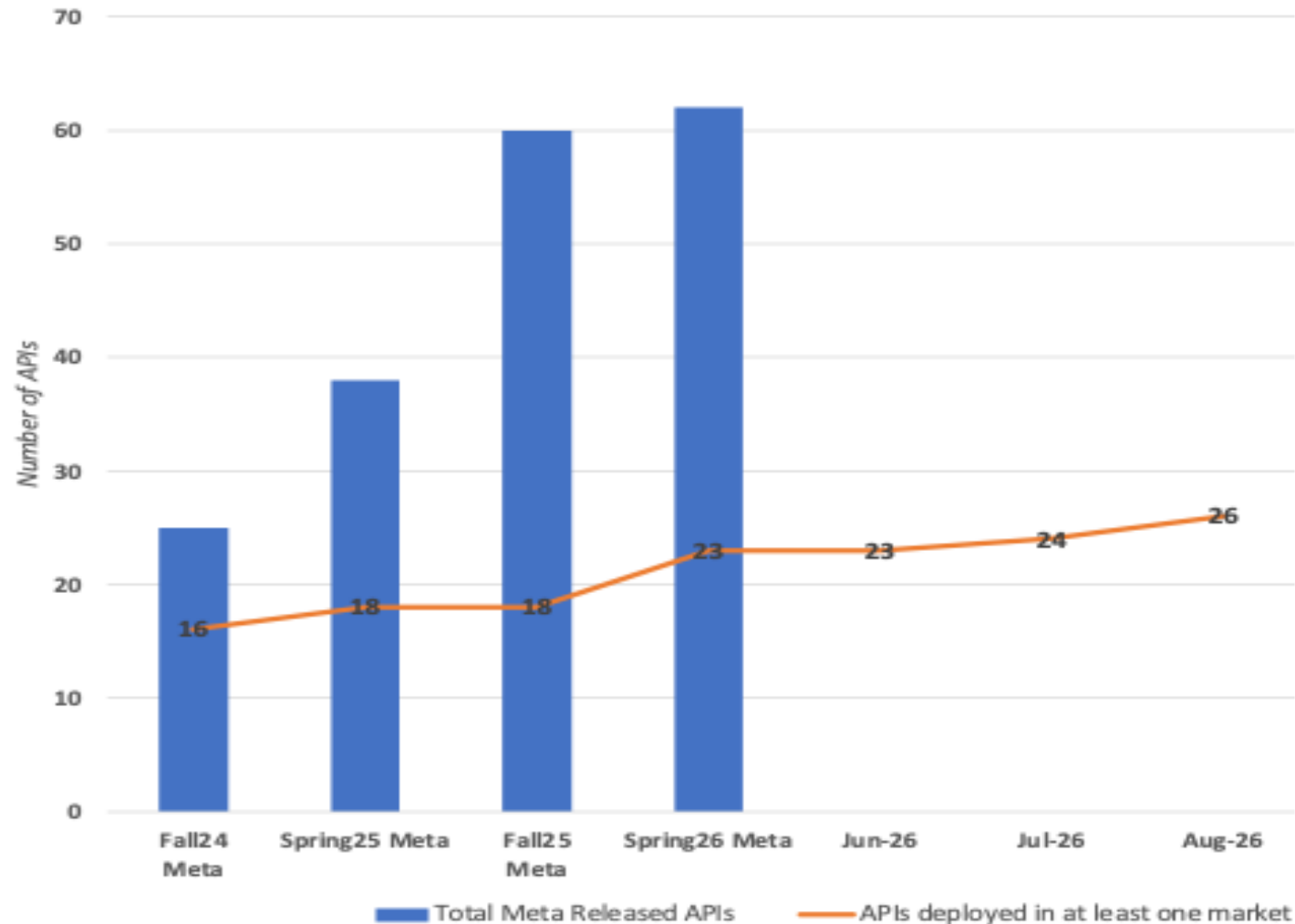
32 market champion launches with align GTM services, engaged with **78** Markets

>60% of mobile connections protected by commercial Anti-Fraud APIs

Open Gateway Market Champion Forecast

<i>GTM Champion Leads</i>	<i>Jill Cooper</i>	<i>Martin W</i>	<i>Alexandra</i>	<i>Hong Lui</i>	<i>Nauman</i>	<i>Ruben</i>	<i>Nauman</i>		
Market Launch Forecast	Europe	Latam	APAC	Greater China	Africa	North America	MENA	Total	Connections
6 Live	8	9	8	2	1	2	2	32	61.4%
4 Q2 2026 (June 2026)	0	0	0	0	0	0	0	0	0.2%
3 Q3 2026 (October Board Meeting)	0	0	2	1	3	0	3	9	5.9%
2 Q4 2026 (EoY 2026)	5	7	2	0	2	0	1	17	6.1%
1 In Progress No Forecast / At Risk	3	2	6	1	3	1	4	20	6.7%
Total	16	18	18	4	9	3	10	78	80.3%
	United Kingdom	Peru	Indonesia	China	South Africa	Canada	UAE		
	France	Chile	Thailand	Taiwan	Uganda	United States	Qatar		
	Spain	Argentina	Sri Lanka	Hong Kong	Cameroon	Bahamas	Oman		
	Germany	Brazil	Singapore	Macau	Nigeria		Saudi Arabia		
	Netherlands	Mexico	Cambodia		Zambia		Egypt		
	Italy	Ecuador	Philippines		Tanzania		Turkiye		
	Poland	Paraguay	Malaysia		Kenya		Morocco		
	Greece	Colombia	India		Cote d'Ivoire		Tunisia		
	Portugal	Uruguay	Australia		Malawi		Kuwait		
	Ireland	El Salvador	New Zealand				Bahrain		
	Belgium	Guatemala	Vietnam						
	Switzerland	Honduras	Japan						
	Austria	Nicaragua	South Korea						
	Romania	Costa Rica	Uzbekistan						
	Sweden	Dominican Rep	Pakistan						
	Hungary	Panama	Bangladesh						
		Bolivia	Mongolia						
		Venezuela	Maldives						

CAMARA API deployment summary



- 26 APIs have now been deployed, i.e. launched by at least one operator
- Two New API deployed in Aug'26
 - *IOT Sim Fraud Prevention*
 - *IOT Sim Fraud Subscription*



Mature API Details can be found at:
<https://www.gsma.com/solutions-and-impact/gsma-open-gateway/gsma-open-gateway-api-descriptions/>

GSMA Open Gateway APIs

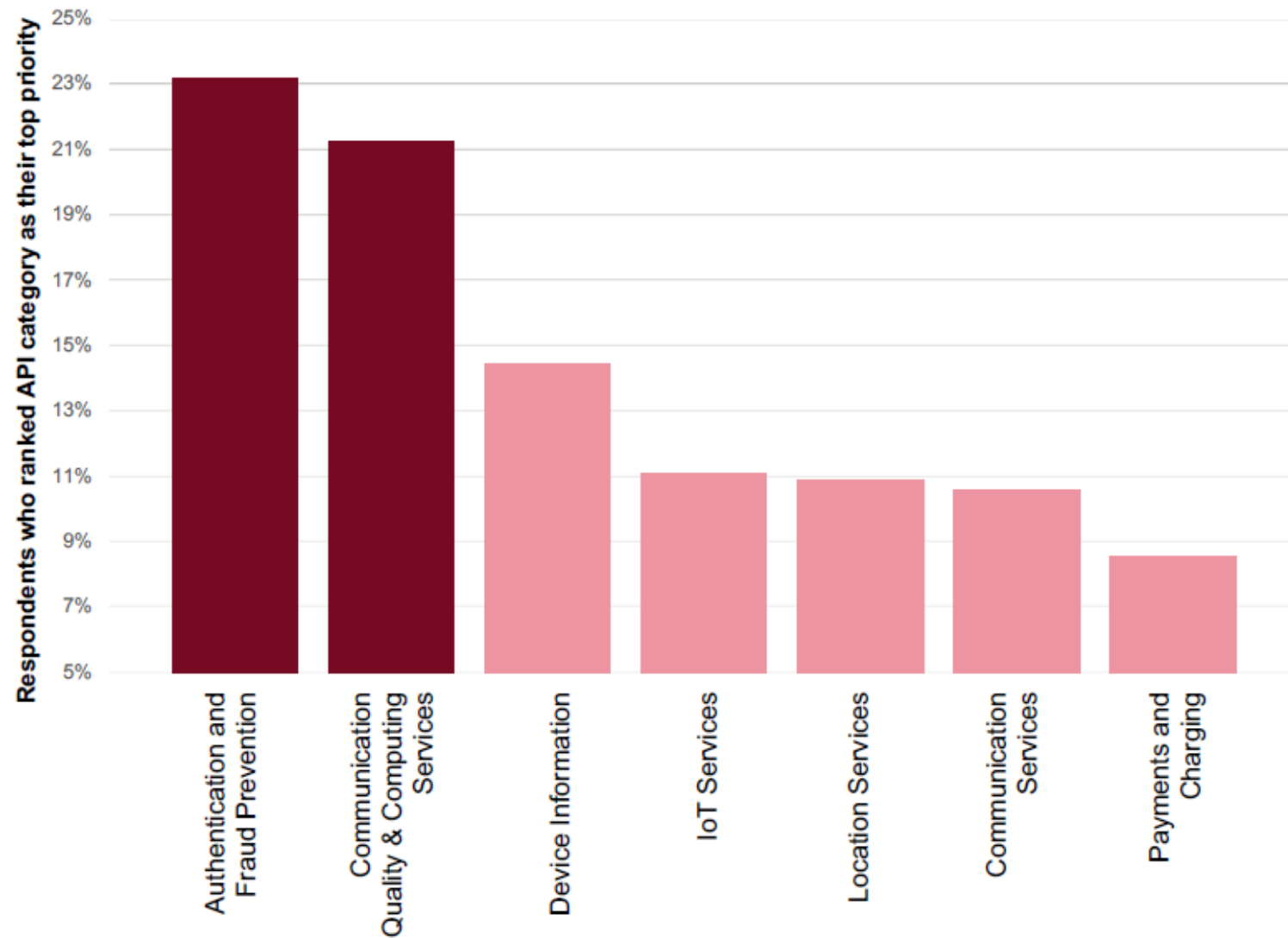
API family					
Authentication and Fraud Prevention	Location Services & Spatial Data	Communication Quality & Slicing	Device Information & Status	Computing & Edge Services	Core Communication, Payments & Management
SIM Swap	Location Verification	Quality on Demand (QoD)	Device Reachability Status	Simple Edge Discovery	Carrier Billing
Number Verification	Location Retrieval	Home Devices QoD	Device Reachability Status Subscriptions	Optimal Edge Discovery	Blockchain Public Address Validation
One-Time Password (OTP) SMS	Device Visit Location	Network Slice Booking	Device Roaming Status	Application Endpoint Discovery	Click-To-Dial
Device Swap	Most Frequent Location	Network Slice Assignment	Connected Network Type Subscriptions	Application Endpoint Registration	Multi-Point VPN
Tenure	Population Density Data	Dedicated Network	Device Identifier	Edge Application Management	SMS (Programmable messaging)
Number Recycling	Region Device Count	Dedicated Network Accesses	Device Data Volume	Traffic Influence	Network Access Management
Know Your Customer (KYC) Age Verification	Brand Registration	Dedicated Network Profiles	Device Data Volume Subscriptions	Energy Footprint Notification	Subscription Status
Know Your Customer (KYC) Fill-In		QoS Booking		MaaS Knowledge Base	Capabilities and Runtime Restrictions
Verified Caller		QoS Booking and Assignment		MaaS QA Assistant (Manage & Service)	Consent Info
IoT SIM Fraud Prevention		Predictive Connectivity Data			
IoT SIM Fraud Prevention Subscriptions					

Source: GSMA Full descriptions are available at [GSMA Open Gateway API Descriptions](#)

CAMARA API progress summary

Region	Authentication and Fraud Prevention												Location Services				Communication Quality		Device Information			Computing Services	Payments and Charging	Total
	Brand Registration	Call Forwarding Signal	Device Status	Device Swap	Home Devices Quality on Demand	IoT SIM Fraud Prevention	IoT SIM Fraud Prevention	KnowYourCustomer	Number Recycling	Number Verification	OTP Validation	SIM Swap	Verified Caller	Device Location Retrieval	Device Location Verification	Population Density Data	Region Device Count	Quality on Demand	Device Identifier	Device Reachability Status	Device Roaming Status	Simple Edge Discovery	Carrier Billing	
APAC	0	0	0	1	0	0	0	1	0	2	0	1	0	0	0	0	0	0	0	0	0	1	0	6
Europe	1	6	5	6	1	0	0	20	2	18	1	22	1	0	5	2	0	1	4	6	6	0	1	108
LATAM	0	0	3	1	1	0	0	4	0	12	1	18	0	4	9	0	0	1	0	0	4	0	0	58
MENA	0	0	2	0	0	0	0	0	0	5	5	8	0	0	0	0	0	0	0	0	0	0	1	21
NA	0	0	2	0	0	0	0	0	0	3	0	5	0	0	1	0	0	1	0	0	0	1	0	13
NE Asia	0	1	4	0	0	1	1	4	1	6	3	6	0	2	5	1	1	2	1	0	3	0	0	42
SE Asia	0	1	0	2	0	0	0	1	0	21	1	11	0	0	4	0	0	1	0	0	2	0	0	44
SSA	0	0	0	0	0	0	0	0	0	6	13	11	0	0	0	0	0	0	0	0	0	0	0	30
South Asia	0	1	0	1	0	0	0	0	1	5	6	5	0	1	2	0	0	0	0	0	1	0	2	25
Total	1	9	16	11	2	1	1	30	4	78	30	87	1	7	26	3	1	6	5	6	16	2	4	347

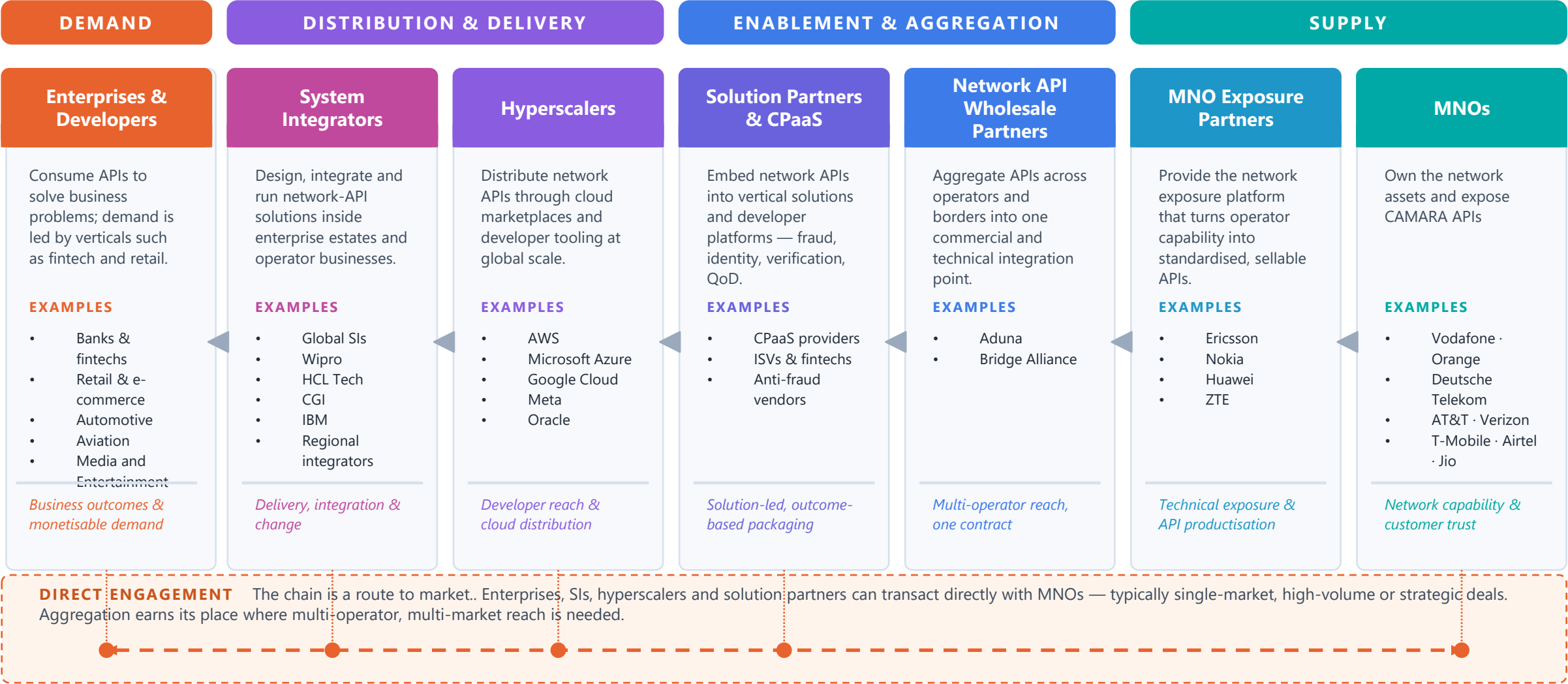
Highest ranked APIs in APAC...



Key CAMARA APIs	
Authentication and Fraud Prevention	Communication Quality & Computing Services
Call Forwarding Signal	QoS Profiles
Device Swap	QoS Provisioning
KYC Age Verification	Quality on Demand
KYC Fill In	Simple edge Discovery
KYC Match	
KYC Tenure	
Number Verification	
OTP SMS	
Scam Signal	
SIM Swap	

Mobile Ecosystem Value Chain — GSMA Open Gateway / Market Gateway

Demand view: how enterprise need is met by network capability — through the chain, or directly with operators



Website for enterprises, developers & resellers to engage

U Mobile Developer Hub

Discover the Unbeatable 5G experience we have for U

You're a step closer to the future with U Mobile. Our Network APIs bring unbeatable capabilities to your solutions, helping you build the next "wow" moment for U and your business. Visit our Developer Hub and start building today.

Visit our Developer Hub and start building today.

[Get Started!](#)

GSMA[®] API Certified



SIM Swap API

Verify users by detecting recent SIM swaps to prevent fraud.

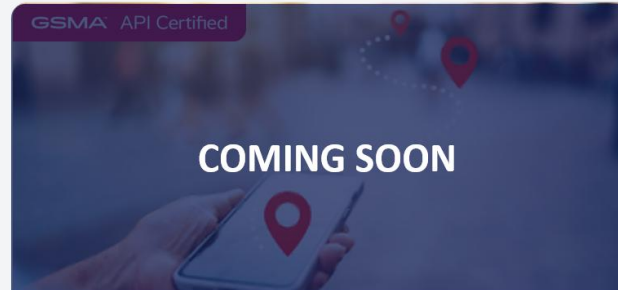
GSMA[®] API Certified



Number Verification API

Ensure the accuracy of users' phone numbers for secure communication.

GSMA[®] API Certified

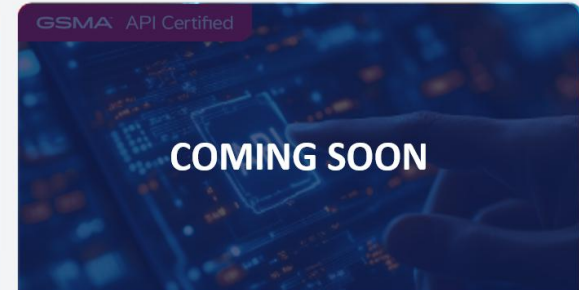


COMING SOON

Device Location

Create, retrieve and delete event subscriptions to realize geofencing for a user device.

GSMA[®] API Certified



COMING SOON

Quality on Demand

Allows the discovery of Quality of Service (QoS) profiles and its characteristics.

Scam & Fraud Problem

Exponential growth in fraud & scams

\$1 Trillion

lost worldwide to scams in 2024¹

50%

of consumers receive scam messages weekly²

25%

of unknown calls are scams³

Source: 1. BioCatch 2025 Global Scams Report, 2. GASA Global State of Scams Report 2025 , 3. Hiya.com

 Malaysia scam losses rise to RM2.7bil in 2025, spike during festive seasons

BUSINESS

Malaysia scam losses rise to RM2.7bil in 2025, spike during festive seasons

Tuesday, 24 Mar 2026 | 10:47 AM MYT

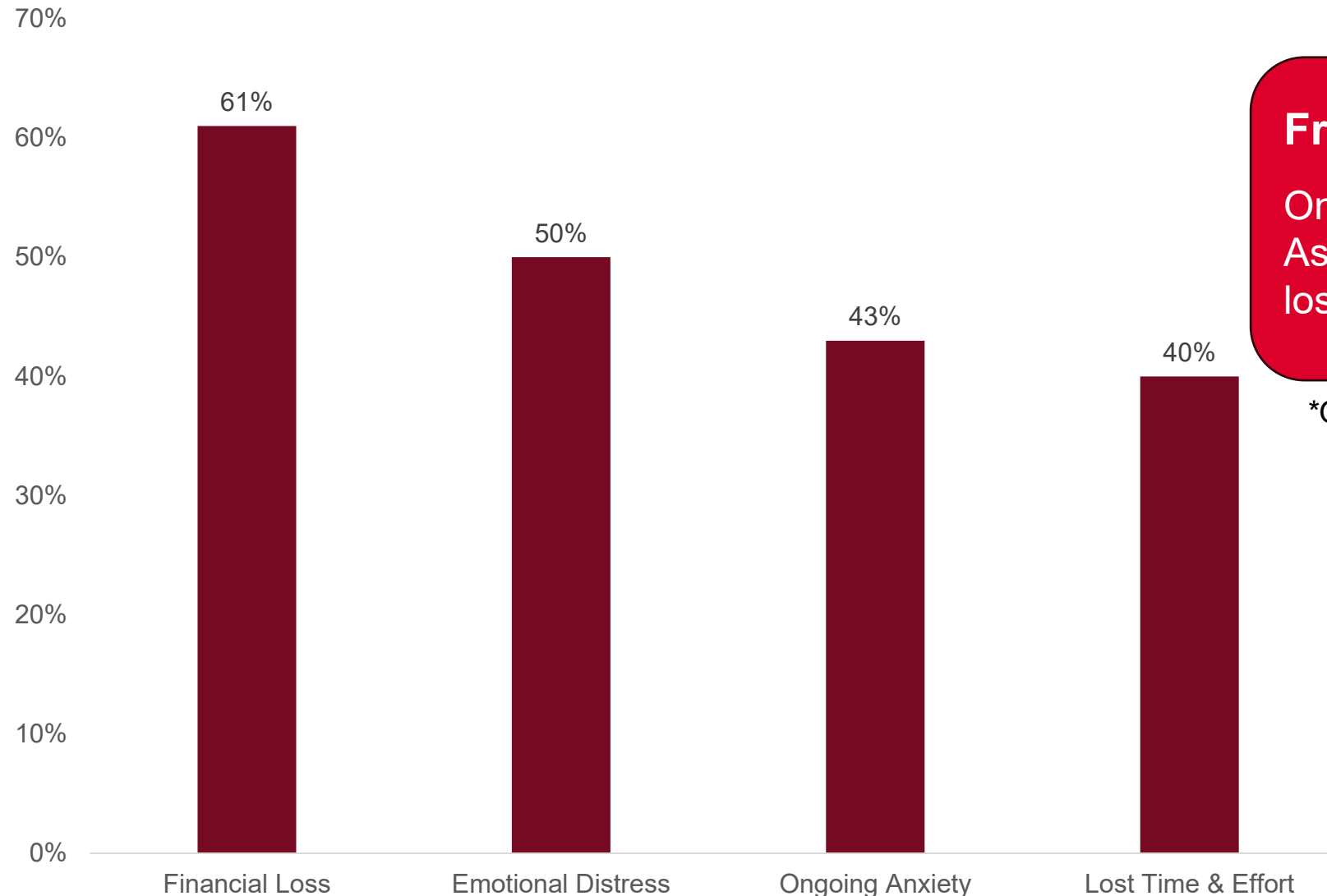
“

Over the last five years, scams have grown massively – they affect more people, occur more often and through more methods. Only by uniting and working together across the digital ecosystem and the financial sector, with the support of public authorities, can we fight such a complex phenomenon. The mobile ecosystem stands ready to do its part, alongside all concerned parties.

Vivek Badrinath, Director General, GSMA



Impact of fraud & scams on digital trust



Fraud Undermines Digital Trust

On average, >50% of scam victims in Asia suffered a significant or complete loss of trust with the internet.*

*Global Anti-Scam Alliance Asia Scam Report 2024

SMS OTP contribution to fraud



A Challenger by Gartner, trusted by you


[GET THE REPORT](#)
[FORTINET](#)

Topics ▾ News ▾ Training ▾ Resources ▾ Events ▾ Jobs ▾

TRENDING: The Cybersecurity Skills Gap and the Role of AI for Defenders • Modernizing at Speed: Scaling AI and Apps Without New Silos •

Account Takeover Fraud, Anti-Phishing, DMARC, Finance & Banking



One-Time Passcodes Are Gateway for Financial Fraud Attacks

Report Reveals Growing Trend of Fraudsters Intercepting SMS-Based Verification

Suparna Goswami (@suparna) • April 3, 2026

[Share](#)
[Post](#)
[Share](#)
[Credit Eligible](#)
[Get Permission](#)



OTP verification is less reliable as fraudsters increasingly exploit SMS-based verification weaknesses to carry out account takeover and payment fraud schemes. (Image: Shutterstock)

Financial institutions have historically relied on one-time passcodes as a primary authentication control for their accountholders. But OTP verification is less reliable as fraudsters increasingly exploit SMS-based verification weaknesses to carry out account takeover and payment fraud schemes.



A Challenger by Gartner, trusted by you

Fortinet is Again Recognized as a Challenger in the 2025 Gartner® Magic Quadrant™ for SIEM

[GET THE REPORT](#)

GET DAILY EMAIL UPDATES

Covering topics in risk management, compliance, fraud, and information security.

Email address

[Submit](#)

By submitting this form you agree to our [Privacy & GDPR Statement](#).

RESOURCES

Why Enterprises Are Flying Blind in the Age of AI Security

The Evolution of Scattered Spider: How Organizations Are Strengthening Defenses

Securing Agentic AI Demands Visibility

Intelligent Banking in the Age of AI: Unifying Fraud, Security, and Compliance



Paul Simpson  • 2nd

Financial Services, Financial Crime, Payments, Mobile Intelligenc...

10mo • 

[+ Follow](#) ...

\$6.7B lost to SMS OTP Fraud Globally in 2023 alone!! UAE begins phasing out SMS & email OTPs for financial transactions. Every Country needs to pay attention. Silent Authentication+ is already available. What is it and why do I need it?! Nothing to intercept by criminals, faster, more secure user authentication, better regulatory compliance, no password, PIN/OTP management or costs...

\$6.7B lost to SMS OTP Fraud Globally in 2023 alone!



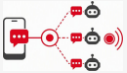
Source: <https://international.itglobal.com/mobile-intelligence>

How common tactics translate into OTP fraud ^{1/2}

Fraud type	The Tactic	The Fraud
Social Engineering (Phishing / Smishing / Vishing) 	Impersonates a bank, telco or support desk; creates urgency and asks the user to read or key in an OTP.	The real OTP is used to approve a login, payment or account takeover in the scammer's session.
SIM Swap / Port-Out 	Uses stolen identity details or social engineering to move the victim's number to a new SIM/eSIM.	SMS OTPs are routed to the attacker, enabling MFA bypass and high-risk transaction approval.
APP scam / payment redirection 	Builds trust and instructs the victim to send funds to a "safe account" or fake invoice, then confirm the OTP.	The victim authorizes a transfer to a mule or scammer account, so the payment appears customer-approved.
Remote Access (Malware / Trojans / APK's) 	Tricks the user into installing an app or granting screen/access permissions that expose OTP prompts.	The attacker hijacks the session and performs transfers or account changes while the OTP is captured or relayed.

Note: high-level typology for fraud awareness; tactics often combine across channels.

How common tactics translate into OTP fraud ^{2/2}

Fraud type	The Tactic	The Fraud
SS7 exploitation 	Abuses telecom signalling weaknesses to intercept or redirect SMS OTP delivery.	Attacker receives the OTP and uses it to complete account login, takeover or payment approval.
Man-in-the-Middle (MitM) 	Spoofs a trusted website or app to capture credentials and OTPs in real time.	The OTP is relayed instantly to access the account or approve a high-risk transfer.
SMS Pumping / AIT 	Uses bots or fake sign-ups to trigger large volumes of OTP SMS to premium or controlled numbers.	Fraudster monetizes termination or traffic fees; the business pays inflated SMS costs without true users.
AI-enhanced deception 	Uses deepfake voice, chatbots or tailored messages to make OTP requests seem legitimate.	Victims are persuaded to reveal OTPs or approve actions they believe are bank-initiated.

Note: high-level typology for fraud awareness; tactics often combine technical compromise and social engineering.

OTP vulnerability is becoming a regulatory issue

Banks Are Ditching OTP Texts By June—Here's How Your Money Stays Safe



Logging into your banking app may look a little different soon. The familiar step of waiting for a one-time password (OTP) via text message could soon disappear, as the **Banko Sentral ng Pilipinas (BSP)** moves to strengthen the country's defenses against online scams.

Philippines

UAE Central Bank Tells FIs to Drop SMS, OTP Authentication

Banking Sector Faces Challenges in Meeting March 2026 Compliance Deadline



The Central Bank of UAE has issued a directive asking financial institutions to eliminate weak authentication methods including SMS and email one-time passwords.

UAE



India



Singapore



Malaysia

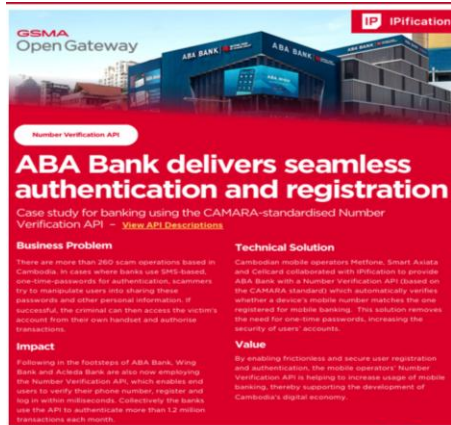
- European regulations: under PSD2 allow OTP use under stricter conditions (ex.dynamic transaction linking and multi-factor requirements).
- U.S. regulators (ic. Federal Financial Institutions Examination Council and Consumer Financial Protection Bureau): view OTPs as a key part of multi-factor authentication under the Gramm-Leach-Bliley Act of 1999.
- Malaysia - BNM RMIT: SMS OTP non-compliant as standalone 2FA since **Nov 2025**

Liability Shift: CBUAE Notice 2025/3057 introduced **financial liability**. If customer's OTP is intercepted or shared during phishing or SIM swap attack, the financial institution is responsible to reimburse the customer for the entire loss. Shifts compliance from a regulatory burden to financial imperative.

Commercial Opportunities

Commercial Case Studies (APAC)

Number Verify/ Silent Network Authentication in Various Verticals



GSMA Open Gateway

Number Verification API

ABA Bank delivers seamless authentication and registration

Case study for banking using the CAMARA-standardised Number Verification API - [View API Descriptions](#)

Business Problem

There are more than 260 scam operations based in Cambodia. In cases where banks use SMS-based, one-time-passwords for authentication, scammers try to persuade users into sharing these passwords and other personal information. If successful, the criminal can then access the victim's account from their own handset and authorize transactions.

Technical Solution

Cambodian mobile operators Metfone, Smart Axiata and Cellcard collaborated with IPification to provide ABA Bank with a Number Verification API based on the CAMARA standard which automatically verifies whether a device's mobile number matches the one registered for mobile banking. This solution removes the need for one-time passwords, increasing the security of users' accounts.

Value

By reducing fraudulence and secure user registration and authentication, the mobile operators' Number Verification API is helping to increase usage of mobile banking, thereby supporting the development of Cambodia's digital economy.

Impact

Following in the footsteps of ABA Bank, Wing Bank and Acleda Bank are also now employing the Number Verification API, which enables and helps to verify their phone number, register and log in without passwords. Collectively the banks use the API to authenticate more than 1.2 million transactions each month.

"The security and convenience of mobile banking is our top priority, and the introduction of IPification will allow us to provide ABA Mobile users with an easier authentication process, keeping the app secure at the same time. The bank will continue bringing the latest developments to the local market, further accelerating the digital transformation throughout the country."

Ashkat Azhikhanov
ABA CEO



CAMBODIA

Challenge:

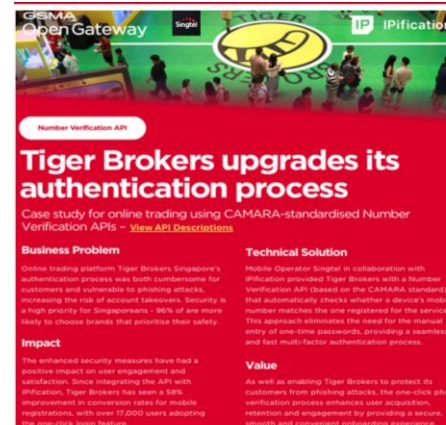
At least **260** scam centers, trafficking an estimated **150,000 foreign** migrant workers. (Cambodia Counter Trafficking in Persons Project)

Solution:

- Metfone, Smart Axiata and Cellcard, collaborated with IPification to **build a common API** that the banking industry can use to fight scams:
 - **Number Verify/ Silent Number Verification** ensuring the device's MSISDN matches the one registered for mobile banking in the background

Results:

ABA, Wing & Acleda Bank: > 1.2 million/ mth transactions



GSMA Open Gateway

Number Verification API

Tiger Brokers upgrades its authentication process

Case study for online trading using CAMARA-standardised Number Verification APIs - [View API Descriptions](#)

Business Problem

Online trading platform Tiger Brokers Singapore's authentication process was both cumbersome for customers and vulnerable to phishing attacks, increasing the risk of account takeovers. Security is a high priority for Singaporeans - 96% of people are likely to choose brands that provide their safety.

Technical Solution

Mobile Operator Singtel in collaboration with IPification provided Tiger Brokers with a Number Verification API (based on the CAMARA standard) that automatically checks whether a device's mobile number matches the one registered for the service. This approach eliminates the need for the manual entry of one-time passwords, providing a seamless and fast multi-factor authentication process.

Value

As well as enabling Tiger Brokers to protect its customers from phishing attacks, the one-click phone verification process enhances user acquisition, retention and engagement by providing a secure, smooth and convenient onboarding experience.

Impact

The enhanced security measures have had a positive impact on user engagement and satisfaction. Since integrating the API with IPification, Tiger Brokers has seen a 58% improvement in conversion rates for mobile registrations, with over 17,000 users adopting the one-click login feature.

"At Tiger Brokers, our commitment to providing a secure and seamless trading experience for our users is paramount. IPification's state-of-the-art phone verification solution significantly enhances our security measures without compromising on user convenience. This partnership reflects our dedication to leveraging innovative technologies to ensure our clients can trade with confidence."

Joe Leong,
CEO of Tiger Brokers Singapore.



SINGAPORE

Challenge:

83.9% of Singaporeans prioritize security over new app features, and **96%** are more likely to choose brands that prioritize their safety. (Appdome survey)

Solution:

- Singtel collaborated with IPification to **build a common API** that the Online Trading industry is using to defend against phishing attacks:
 - **Number Verify/ Silent Number Verification** ensuring device's MSISDN matches the one registered for mobile trading service in the background enhancing both security and user convenience

Results:

Tiger Brokers: 58% improvement in conversion rates (mobile registrations) & 17k users (one-click login feature)



GSMA Open Gateway

Number Verification API

BRI Bank reduces fraud by verifying phone numbers

Case study for banking using the CAMARA standardised Number Verification API - [View API Descriptions](#)

Business Problem

To authenticate customers, banks in Indonesia had been relying on SMS-based, one-time passwords, which are vulnerable to social engineering. If a scammer successfully manipulates a user into sharing these passwords, they may be able to access the victim's account from their own handset and authorize transactions.

Technical Solution

Mobile operators Telkomsel, XL Smart and IOH provided BRI Bank with the CAMARA-based Number Verification API, which automatically verifies whether a device's mobile number matches the one registered for mobile banking. Working in the background, this automated solution removes the need for one-time passwords, increasing the security of users' accounts.

Value

The Number Verification API provides enterprises with a trusted authentication method, strengthening Indonesian mobile operators' position in the fast-growing digital identity market.

Impact

BRI Bank reports a 70% reduction in social engineering incidents across its mobile apps. It has also seen a 20% improvement in the rate of successful authentications versus SMS-based one-time passwords, while the average time it takes for users to log into the app has halved.

"Number Verification is not just an alternative to SMS one-time-passwords, it's a better model: invisible to users, resistant to social engineering and tampering, and trusted by security-conscious industries. For mobile operators, consistent network APIs can support strategic collaboration with hyperscalers and fintech, helping them reclaim relevance and revenue in the authentication ecosystem."

Telkomsel



INDONESIA

Challenge:

361 Mio Cyber Attack Threats in Indonesia in the 1st 10 months of 2023 (BSSN 2023)

Solution:

- Telkomsel, XL Smart and IOH collaborated with BRI Bank to **build a common API** that the banking industry can use to fight scams:
 - **Number Verify/ Silent Number Verification** ensuring the device's MSISDN matches the one registered for mobile banking in the background

Results:

BRI Bank: the Reduction in Social Engineering in BRIMo apps by 70% and 20% improvement in successful authentication.



GSMA Open Gateway

Number Verification API

EASY BUY verifies phone numbers to secure transactions

Case study for payments using the CAMARA-standardised Number Verification API - [View API Descriptions](#)

Business Problem

Financial fraud in Thailand is a major issue. According to the Royal Thai Police, losses totalled 63 billion baht (US\$1.9 billion) across 540,000 victims between March 2022 and May 2024. Part of the problem is the vulnerability of one-time passwords, which are used to authenticate transactions, to phishing attacks by fraudsters.

Technical Solution

Mobile operator True Business is employing the CAMARA-based Number Verification API to enable EASY BUY, a financial services provider, to seamlessly authenticate a mobile transaction on its Umay+ application. By verifying True-dtac mobile numbers, the Number Verification API removes the need to use SMS one-time passwords in the verification process.

Value

By helping to automatically verify identities and increase security, the Number Verification API can simplify a range of transaction processes including online applications, money transfers, credit limit increases, and cash withdrawals.

Impact

The Number Verification API is helping to protect the 1.5 million active users of the Umay+ application, which handles more than 1.5 million transactions per month. As well as simplifying the mobile transaction process and enhancing customer experience, the solution provides a high level of security.

"In collaboration with TrueBusiness, EASY BUY has adopted the cutting-edge Number Verification API technology. This simplifies transaction processes while ensuring security and reliability against fraudulent activities. This milestone marks EASY BUY as Thailand's first financial service provider implementing Number Verification API technology to upgrade security, improve service quality, build greater customer confidence, and strengthen our competitive edge in the financial services industry."

Nuchal Kattakorn, EVP of Business Planning Department, Customer Service Department and Operation Centre, EASY BUY Pte



THAILAND

Challenge:

The financial fraud damage totaled **63 billion baht (US\$1.9billion)** with **540,000** victims between March 2022 and May 2024. (Royal Thai Police Report)

Solution:

- True-Dtac collaborated with EASY BUY to **build a common API** that the financial service industry use to simplify transactions like online application activation, money transfers, credit limit increases and cash withdrawals thru their Umay+ app:
 - **Number Verify/ Silent Number Verification** ensuring the device's MSISDN matches the one registered for mobile banking in the background

Results:

EASY BUY: protect 1.5mil active Umay+ users with 1.5mil transactions per month.



Besides security, number verify also addresses...



Number Verify is a security and experience upgrade

not an SMS replacement

It strengthens authentication while removing the OTP step from the customer journey.



AUTH SUCCESS

99% vs ~80%
SMS

Fewer failed authentications and fewer drop-offs.



LOGIN AUTH TIME

8 sec vs 19 sec
SMS

Shorter login authentication use case.



USER EXPERIENCE

Zero
user friction

No code to copy, no app switching, fewer interruptions.

Value equation

Reduced
fraud

+

Higher
conversion

+

Compliance

+

Better CX

=

**stronger trust +
less customer effort**

NV performance points supplied for discussion; exact outcomes depend on implementation and market coverage.

Source: InfoBin – Velid Kasapovic, 14th May 2026: From Capability to Revenue (Implementation in Brazil) & FIDO Alliance Survey (for Auth Success (up to 20% SMS Fail to arrive)

SMS OTP vs number verify demo

SMS OTP verifies a user-entered code; Number Verify validates the mobile number silently through the operator network.

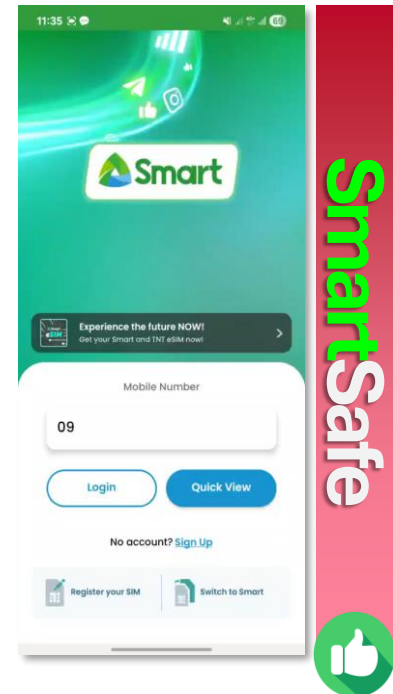
OTP Authentication

- 1 **Start Your Transfer**
Open the app and select the Fund Transfer option.
- 2 **Enter Details**
Input the amount and destination account.
- 3 **OTP Sent**
The app sends a one-time password to your mobile number.
- 4 **Check SMS**
Open your messages to find the OTP.
- 5 **Enter OTP**
Retrieve the OTP from SMS and input it in the app.
- 6 **Complete Transfer**
Once verified, your funds are successfully sent.

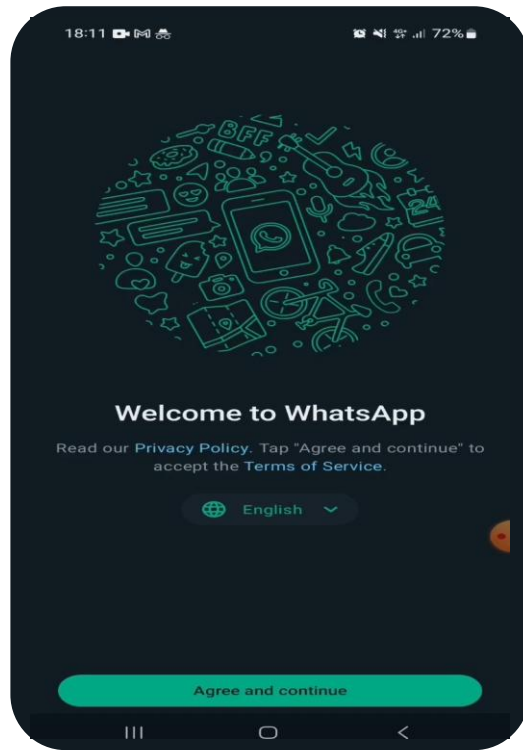


SmartSafe SilentAccess

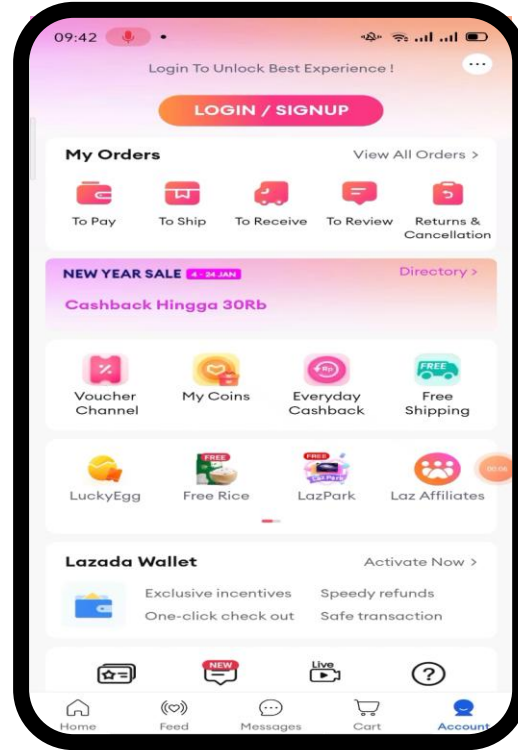
- 1 **Start Your Transfer**
Open the app and select the Fund Transfer option.
- 2 **Enter Details**
Input the amount and destination account.
- 3 **We've got you covered**
The Silent Authentication system checks your mobile number in the background—no codes, no input.
- 4 **Complete Transfer**
Once verified, your funds are successfully sent.



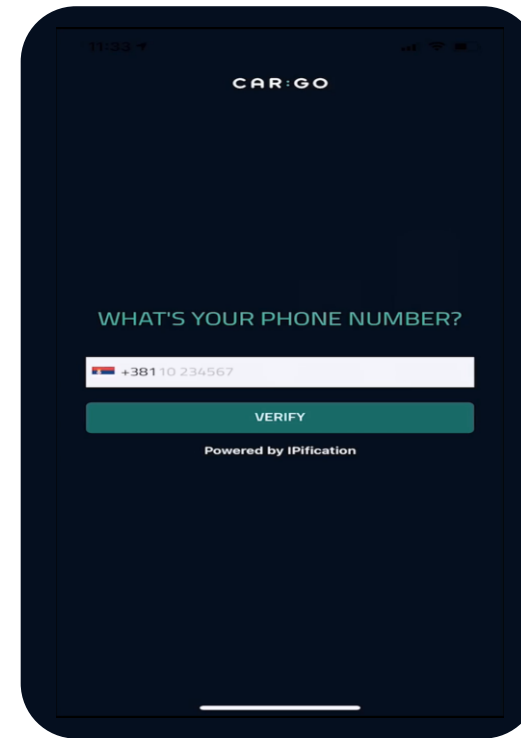
Various industries are potential users of number verify



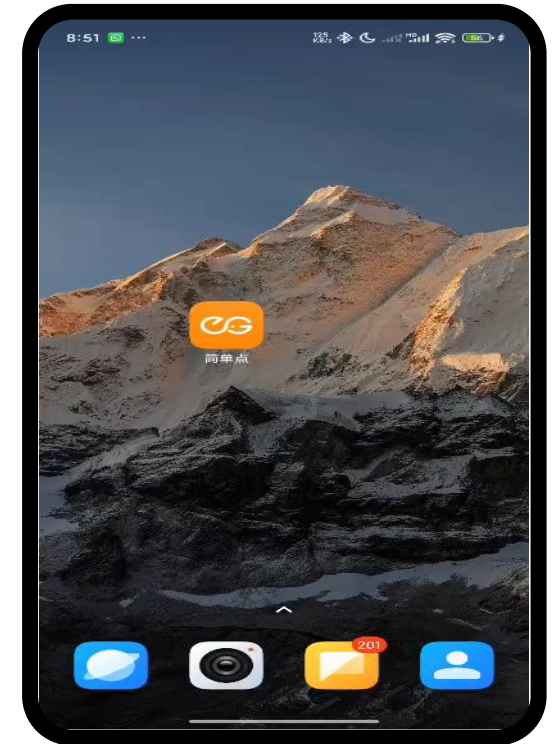
Social App - Meta



M-Commerce - Lazada



Ride Hailing App - CarGo



Food Delivery App – E-Gets

Commercial Case Studies

Infobip: Device Location – Bank in Brazil (BancoDaycoval)



The graphic features a blue header with the GSMA Open Gateway logo and a photo of the Banco Daycoval building. Below is a red section with white text detailing the case study. The title is 'Banco Daycoval taps location data to reduce fraud'. It includes sections for Business Problem, Technical Solution, Value, and Impact. A quote from Alexandre Rhein, CIO of Daycoval Bank, is at the bottom left, and a circular portrait of him is at the bottom right.

GSMA Open Gateway

BancoDaycoval

Location Verification API

Banco Daycoval taps location data to reduce fraud

Case study for banking using the CAMARA-standardised Location Verification API - [View API Descriptions](#)

Business Problem

In Brazil, US \$54 billion is lost to scams each year, according to the Global Anti Scam Alliance. When an individual tries to open a new account or take out a loan, banks need to assess the risk of fraud. A key factor to check is whether the applicant's location is consistent with the home address they provide.

Impact

The Location Verification API can reliably verify the geographic position of a device, without the need for GPS, which is vulnerable to spoofing. In a matter of seconds, Daycoval has the data it needs to make a risk assessment on the loan application.

Technical Solution

Mobile operators Vivo, Claro and TIM collaborated with Infobip to provide banks with CAMARA-based APIs that can be used to counter scams. Banco Daycoval has integrated the Location Verification API into its application process. The bank now asks applicants whether they consent to sharing their location with Banco Daycoval, which then uses network data to check whether the address is consistent with the device's location.

Value

By lowering Brazilian banks' exposure to fraud, the Location Verification API is reducing the cost of providing credit to individuals. As well as helping consumers borrow money when they need it, a well-functioning financial services system can fuel economic growth.

"The API Device Location verification represents a technological advancement, as it provides superior precision in real-time of customer location compared to current public standards ... Vivo, once again, brings innovation to our products. I see this as an opportunity to test and implement new solutions, which will further enhance the robustness of our process and the precision of our decisions."

Alexandre Rhein
CIO of Daycoval Bank

BRAZIL

Challenge:

\$54 billion lost to scams in Brazil
(State of Scams in Brazil, GASA)

Solution:

- Vivo, Claro & TIM collaborated with Infobip **to build a common set of APIs** that the banking industry can use to fight scams/identity theft:
 - **Device Location** identifies the geographical location of the user's device without GPS (vulnerable to spoofing)

Results:

Banco Daycoval: reduced the cost to providing credit to individuals & allowing on-demand borrowing by consumers

Commercial Case Studies

Infobip: SIM Swap API – Bank in Brazil (Itaú)



The image shows a promotional graphic for the Infobip SIM Swap API. At the top left, it says 'GSMA Open Gateway'. In the center, there's a red banner with the text 'SIM Swap API'. Below this, the main headline reads 'Itaú Bank combats payment scams'. Underneath the headline, it says 'Case study for bank payments using the CAMARA-standardised SIM Swap API - [View API Descriptions](#)'. The graphic is divided into three columns: 'Business Problem', 'Technical Solution', and 'Impact'. The 'Business Problem' column states that in Brazil, most banking transactions are now conducted through digital channels, which are vulnerable to fraud, where attackers use stolen personal data and social engineering to hijack a user's SIM card and take control of their account. About US\$54 billion is lost to scams in Brazil each year according to the Global Anti Scam Alliance. The 'Technical Solution' column explains that to help authenticate payments, Itaú Bank, working with aggregator Infobip, is employing the SIM Swap API to source a date and time stamp showing when a SIM associated with a phone number was last changed. The API is one of several CAMARA-based network APIs launched in a coordinated effort by mobile network operators Claro, TIM and Vivo in Brazil. The 'Impact' column states that Itaú Bank can now detect SIM card swaps easily and quickly, identifying potential fraud and providing an extra layer of protection for its users. In March 2024, Claro alone processed three million SIM Swap APIs.

Business Problem

In Brazil, most banking transactions are now conducted through digital channels. These transactions are vulnerable to fraud, where attackers use stolen personal data and social engineering to hijack a user's SIM card and take control of their account. About US\$54 billion is lost to scams in Brazil each year according to the Global Anti Scam Alliance.

Technical Solution

To help authenticate payments, Itaú Bank, working with aggregator Infobip, is employing the SIM Swap API to source a date and time stamp showing when a SIM associated with a phone number was last changed. The API is one of several CAMARA-based network APIs launched in a coordinated effort by mobile network operators Claro, TIM and Vivo in Brazil.

Impact

Itaú Bank can now detect SIM card swaps easily and quickly, identifying potential fraud and providing an extra layer of protection for its users. In March 2024, Claro alone processed three million SIM Swap APIs.

"We are really proud to be the first financial institution worldwide to leverage the Open Gateway APIs to help us combat fraud through enhanced authentication mechanisms, device location tracking and SIM swap control... We do believe the use case goes beyond bank fraud scenarios and will really improve the customer experience. Open Gateway with our digital transformation strategy will enable us to better serve our customers and advance our vision of a more connected and secure banking ecosystem."

Fábio Napoli
Chief Technology Officer of Itaú Bank



BRAZIL

Challenge:

Most banking transactions are now using digital channels - **87%** growth in online fraud in 2023
(Annual Business & Consumer Fraud Report, AEECF 2023)

Solution:

- Vivo, Claro & TIM collaborated with Infobip to build a **common set of APIs** that the banking industry can use to fight scams/identity theft:
 - **SIM Swap check** identifies if the SIM linked to the mobile number has been recently changed

Results:

Itaú Bank: In Mar 2024, Claro alone processed 3mil SIM Swap API's

Commercial Case Studies

Telefonica: KYC Match – Transport & Logistics in Brazil (Frete)



GSMA
Open Gateway

Know Your Customer Match API

Frete.com verifies the identity of road haulage drivers

Case study for road haulage authentication using the CAMARA-standardised Know Your Customer Match API - [View API Descriptions](#)

Business Problem

Brazil relies heavily on road freight. To serve this market, Frete.com, the largest road haulage company in Latin America, provides drivers that ship more than US\$402 billion worth of freight each year, on behalf of 18,000 companies. To reduce the risk of fraud, Frete.com needs to verify the identity of each of the 900,000 drivers working through the platform.

Impact

By ensuring that a driver is who they say they are, the network APIs are reducing fraud for Frete.com, which pays more than US\$20 billion to drivers each year.

Technical Solution

Vonage, Telefónica and Vivo have together built a common set of APIs that the e-commerce, transport and logistic industries can use to fight scams and identity fraud. Frete.com is now employing the CAMARA-based Know Your Customer Match API to validate the identity of drivers during its authentication process. It verifies the driver's Brazilian ID card and mobile phone number against the mobile operator's data.

Value

As Frete.com can now safely tap a wider pool of trusted drivers, the API-based authentication solution is helping to ensure road freight is transported in a timely and efficient manner. The solution is also easy to deploy: developers can integrate the Know Your Customer Match API into their applications without the need for custom implementations, simplifying processes and reducing time to market.

"In the transport sector, ensuring quality service requires prioritising security, agility and efficiency. Today we face the constant challenge of online identity fraud, a threat that we must address effectively. In this context, the Know Your Customer-Match API emerges as an outstanding solution, offering a way to mitigate this risk and strengthen integrity."

Frete.com



BRAZIL

Challenge:

Road Freight accounts for **67%** of total goods moved in Brazil with **900,000** drivers.

(Informe ICEX 2023 infraestructuras de transporte en Brasil)

Frete in Latin America carries goods worth **US\$402 billion** each year on behalf of **18k** companies.

Solution:

- Telefonica, Vonage & Telefonica, Vivo collaborated to build a common set of APIs that the Transport & Logistic industry use to fight scams/identity fraud:
 - **KYC-Match** validates the identity of the user registered, verifying the Brazilian ID Card (CPF) & mobile phone #

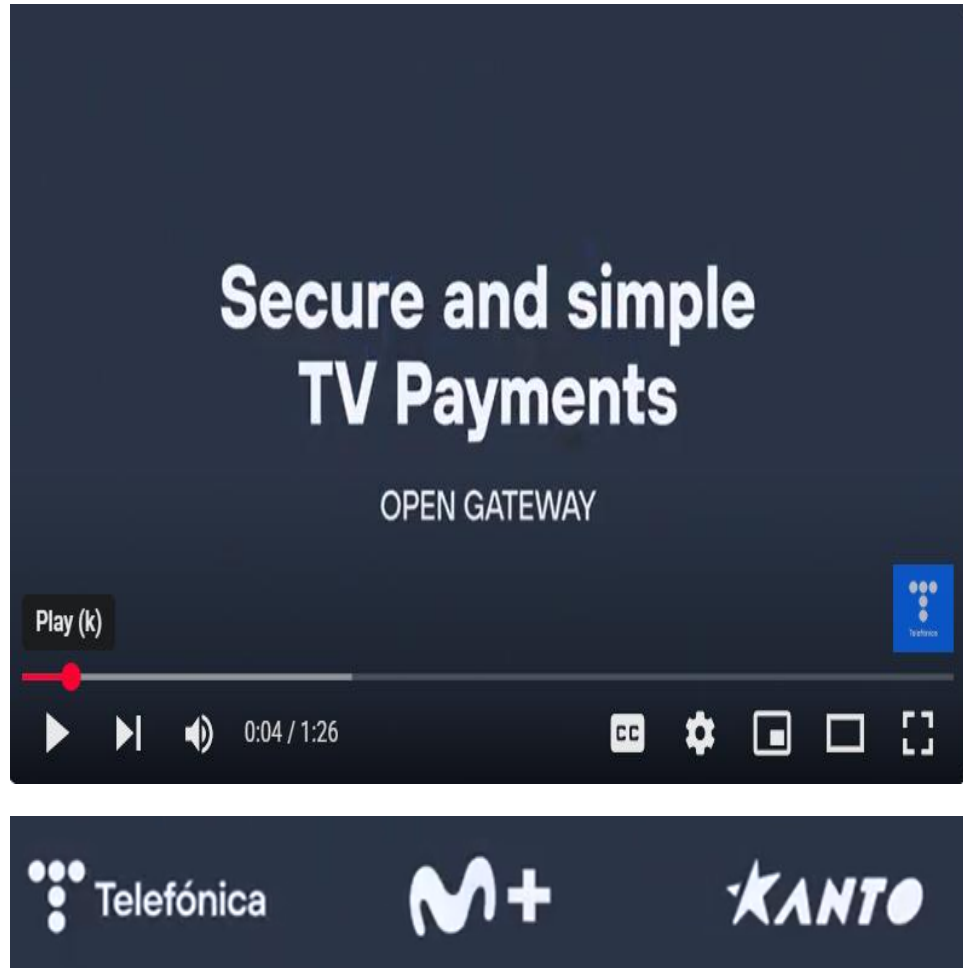
Results:

Frete: reduction in scam by drivers (US\$20 billion/ year to drivers).

GSMA™

Commercial Case Studies

Telefonica: Carrier Billing – Entertainment & e-Commerce Provider Kanto in Spain



SPAIN

Challenge:

Over **75%** of customers would like to shop online through their TV for digital services like games, apps, e-books, music or subscriptions to streaming services
(Source??)

Solution:

- Telefonica and Movistar Plus+ collaborated **to build a common API** that the Entertainment and e-Commerce industry use to simplify the user experience:
 - **Carrier Billing** allows for users to use their mobile subscription to purchase digital services without the need for credit card details and be billed on their mobile

Results:

Kanto: TBA

Commercial Case Studies (Global)

Communications Quality – Gaming & Entertainment (Broadcasting), Unified Comms & Collabs, Health & Wellness

Gaming & Entertainment

Cloud Gaming

Blacknut is a cloud gaming service that provides subscribers unlimited access to 500+ games and cross-device capability for any connected device.

Challenge

Gamers need stable connectivity in key moments, and lag, jitter and buffering are substantial issues that Blacknut wanted to erase from their gamers experience.

Blacknut



Solution

With Vonage, we implemented Quality on Demand to activate higher quality gaming. Now Blacknut's users can enjoy a solid speed, super-fast response times, ultra-low latency and unwavering connectivity, providing a superior experience.

Partner



Open Gateway API

QoD Mobile

Health & Wellness

XR remote surgery

ApoQlar's VSI HoloMedicine is a medical software platform with a feature that constructs a volumetric 3D image based on real world patient scans, which a physician can remotely view using the HoloLens.

Challenge

ApoQlar required solid connectivity as the rendering of the volumetric 3D model relies on a highly reliable connection with stable latency and bandwidth.

apoQlar



Solution

Utilizing Microsoft's HoloLens hardware, we integrated our QoD API in order to guarantee the quality of rendering of the 3D images.

This improves the video, with no image freeze and better resolution, providing a consistent experience for the doctor preparing for surgery.

Partner



Open Gateway API

QoD Mobile

Unified Comms & Collabs

Online Video training

Zoom is a video room service that provides different comms services for work meetings, simultaneous virtual rooms and webinars.

Challenge

Zoom is exploring charging users for higher network quality and/or offering premium services solutions with higher quality to increase the number of paying customers.

zoom



Solution

Integrating Quality on Demand with Vonage, we were able to vastly improve the virtual education experience.

Our solution enables webinar hosts to activate HD mode to ensure the quality of presentations automatically and stabilize connectivity.

Partner



Open Gateway API

QoD Mobile

Industry 4.0

AI Video production

Cinfo is a company specializing in artificial intelligence, 5G, video technologies with a vision to democratize the production of all kinds of events.

Challenge

Cinfo wanted to create an affordable system for high quality broadcasting, using AI in order to simplify workflow and reduce errors and costs. These solutions are highly sensitive to connectivity, quality parameters latency and jitters.

cinfo



Solution

In collaboration with AWS, we deployed our QoD API for their AI to process the frames at the capturing stream FPS rate, during a live event. The result is a live sports broadcast, captured using AI, with no video freeze and no pixel or frame loss.

Partner

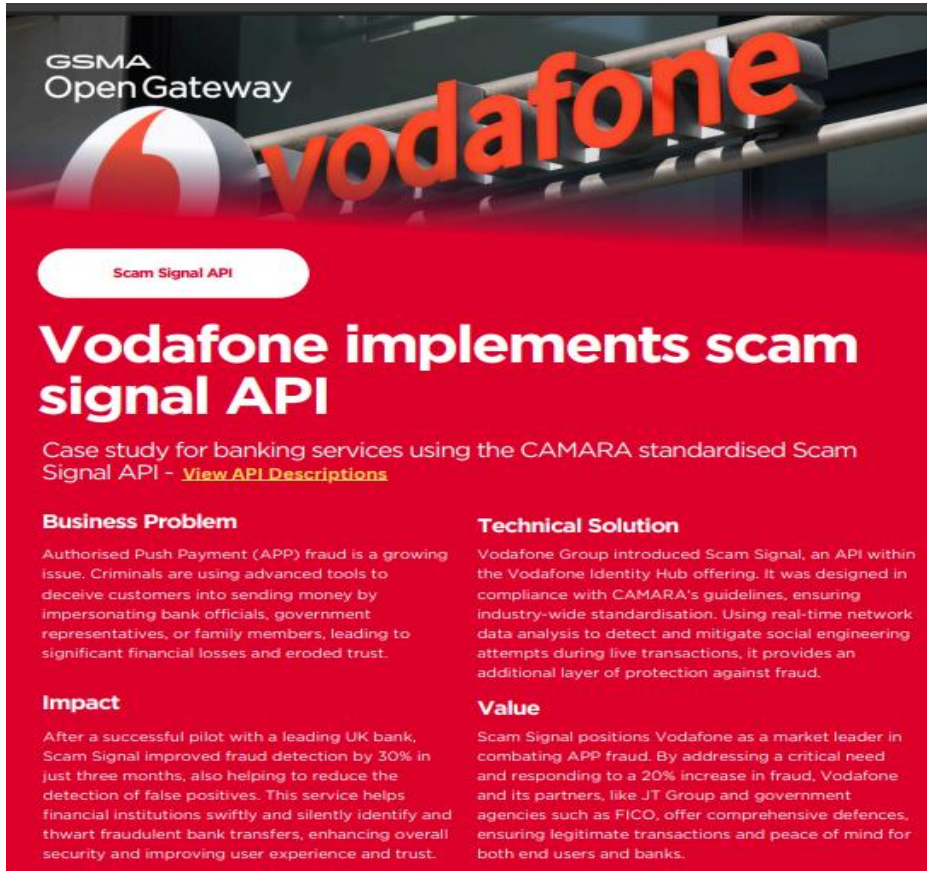


Open Gateway API

QoD Mobile

Commercial Case Studies

Vodafone with FICO & Jersey Telecom : Scam Signal – Financial Institutions



GSMA Open Gateway

Scam Signal API

Vodafone implements scam signal API

Case study for banking services using the CAMARA standardised Scam Signal API - [View API Descriptions](#)

Business Problem Authorised Push Payment (APP) fraud is a growing issue. Criminals are using advanced tools to deceive customers into sending money by impersonating bank officials, government representatives, or family members, leading to significant financial losses and eroded trust.	Technical Solution Vodafone Group introduced Scam Signal, an API within the Vodafone Identity Hub offering. It was designed in compliance with CAMARA's guidelines, ensuring industry-wide standardisation. Using real-time network data analysis to detect and mitigate social engineering attempts during live transactions, it provides an additional layer of protection against fraud.
Impact After a successful pilot with a leading UK bank, Scam Signal improved fraud detection by 30% in just three months, also helping to reduce the detection of false positives. This service helps financial institutions swiftly and silently identify and thwart fraudulent bank transfers, enhancing overall security and improving user experience and trust.	Value Scam Signal positions Vodafone as a market leader in combating APP fraud. By addressing a critical need and responding to a 20% increase in fraud, Vodafone and its partners, like JT Group and government agencies such as FICO, offer comprehensive defences, ensuring legitimate transactions and peace of mind for both end users and banks.

"The threat of social engineering is becoming increasingly sophisticated. The Scam Signal API is an exceptionally effective tool, utilising real-time network data to help banks detect and prevent fraudulent transactions with a very low rate of false positives."

Johanna Wood
Network API Director



UK

Challenge:

Authorized Push Payment (APP) fraud is a growing issue. Criminals are using advanced tools to deceive customers into sending money by impersonating bank officials, government representatives or family members, leading to significant financial losses and eroded trust.

Solution:

- Vodafone Identity Hub offering designed in compliance with CAMARA's guidelines, ensuring industry-wide standardisation:
 - **Scam Signal** uses real-time network data analysis to detect and mitigate social engineering attempts during live transaction, provides additional layer of fraud protection.

Results:

UK bank: Improved fraud detection by 30% in 3 months. Also, detection of false positives. Resulting in better user experience &

GSMA™

Fusion

Fusion focus in 2026...

Building the enterprise demand
evidence base

16 MDIs published

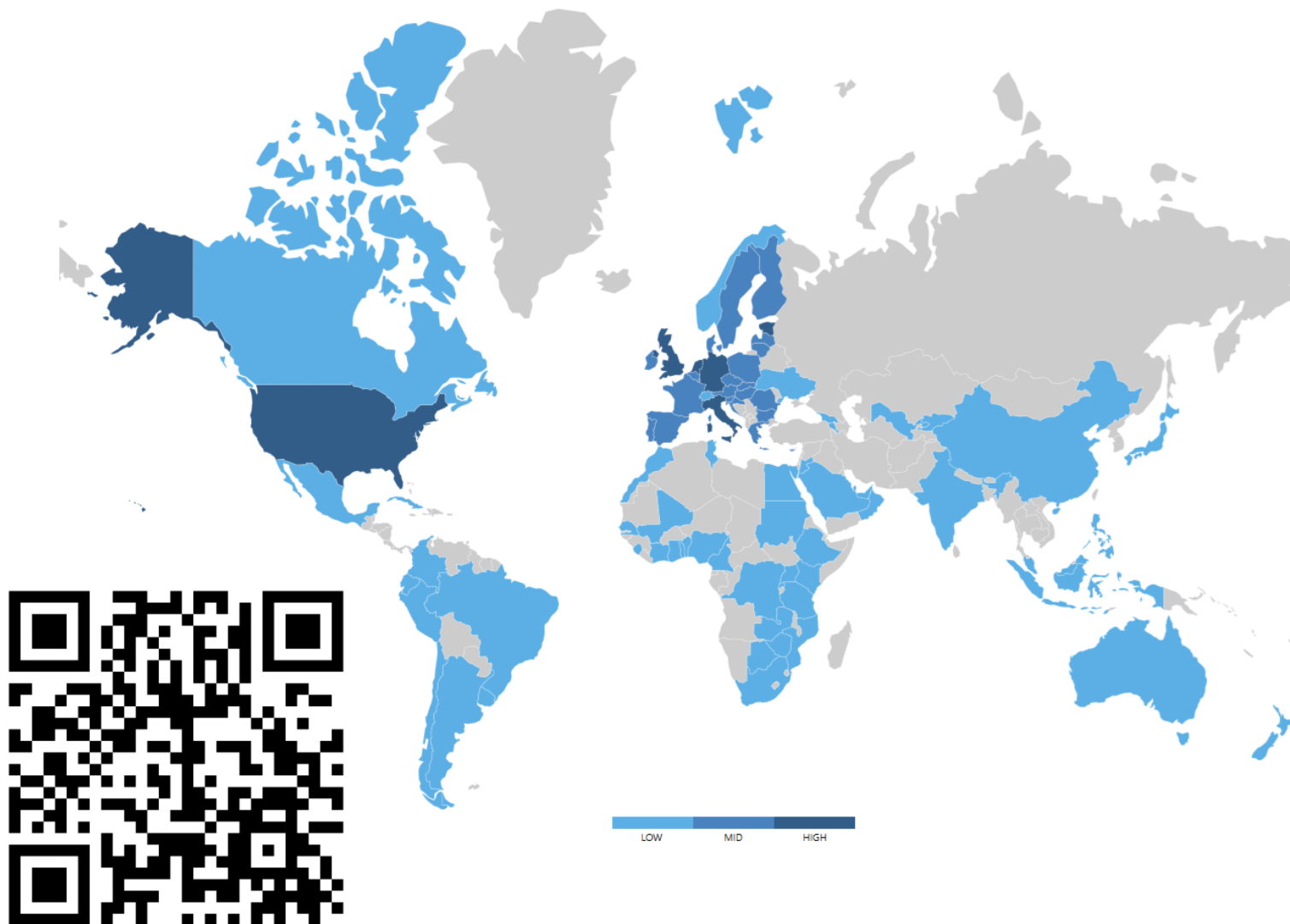
2 Joint Industry Statements of
Requirements.

7 Anti-fraud published
(surpassed stretch target)

9 Comms Quality published

Verticals represented:
Aviation,
Automotive,
Financial Services,
Media & Entertainment,
Retail

Demand map



Individual Market Demand Indicators

34

FICO: Antifraud - Scam Signal API starting with 15 markets in EU, LATAM and APAC.

Skydio: Drone 1st Response QoD API

Tata Elxsi: Automotive & Drones QoD API

JT Global: Age Verification across 6 Markets

Air Europa: QoD across 7 EU, USA and 8 Latam

Flock Safety: QoD Public Safety across United States

Neutral Wireless: QoS + Profile across 5 Markets

IDEMIA: QoD Baggage Identification & Recovery across Saudi, Oz, NZ, USA

IDEMIA: Public-Security-Biometric: Public QoD across 6 Markets

Veloce: eSports QoD Across 12 Markets

Ektar Technologies: Number Verify 2, Sim Swap, Device Identifier and Device Change, KYC Tenure and KYC Match, Location Verification across GCC and Asia

D8Corporation: SIM Swap, Number Verification, KYC Match, Device Location Verification, Device Roaming Status and Device Identifier across 13 markets

Unscammed: SIM Swap, SIM Swap Subscriptions, Number Verification, Call Forwarding Signal, Scam Signal, Number Recycling, Device Swap, Device Roaming Status, Subscription Status, Location Verification, Location Retrieval and Device Identifier across 8 markets

Coure Technologies: Number Verification, Number Recycle, Device Swap, SIM Swap, KYC Customer Match, Scam Signal across 21 African countries

JOINT Market Demand Indicators

Drones e-Conspicuity (QoD, Location Verification, Fraud, Identity & Authentication, Population Density Across USA, UK and EU) with NCSC UK, Barcelona Drone Center, Ericsson, Nokia, NextNav, Dimetor, Shabodi, Invicsa

Vydens: Geofencing Subscriptions, Device Location Verification and Most Frequent Location APIs across Latin America, Europe, Asia Pacific and North America with 3 large Brazilian enterprises Savegnago Supermercados, Fast Shop (and Multiplan who have authorised citation stating commercial interest

Turning enterprise demand to investable operator opportunities

1. Demand Intelligence & Ecosystem Activation:

Vertical scope: Aviation, Automotive, Media, Gaming, FinTech, Retail

Validated demand and ecosystem commitment translated into investable operator opportunities

2. Market Validation:

Market validation activities (trials, pilots or structured validation exercises) converting demand statements into evidence of technical feasibility, business value and commercial readiness

3. Future Networks Requirements:

Bringing enterprise demand into the future networks conversation

Strategic Pivot: expanding from APIs to broader 5G/6G Priority



GSMA™

Thank you

Commercial Case Studies

Orange: Location Verification & QoD – Manufacturing in MWCB (Shabodi)

The graphic features a dark blue header with the GSMA Open Gateway logo, a stylized tree logo for Shabodi, and the Orange logo. Below the header, two white buttons labeled 'Location Verification API' and 'Quality on Demand API' are shown. The main title 'Orange and Shabodi demonstrate how 5G can transform manufacturing' is in large white text. Below it, a subtitle reads 'Case study for manufacturing using the CAMARA-standardised Location Verification and Quality on Demand APIs - [View API Descriptions](#)'. The content is divided into three columns: 'Business Problem', 'Technical Solution', and 'Impact'. The 'Business Problem' column describes the need for reliable connectivity for demanding digital applications. The 'Technical Solution' column describes the use of CAMARA-based APIs to monitor conditions in factories. The 'Impact' column describes the improvement in efficiency and performance in manufacturing environments. A quote from Harpreet Geeke, Co-Founder & CTO of Shabodi, is at the bottom left. A circular portrait of Harpreet Geeke is at the bottom right.

GSMA Open Gateway

shabodi

orange™

Location Verification API

Quality on Demand API

Orange and Shabodi demonstrate how 5G can transform manufacturing

Case study for manufacturing using the CAMARA-standardised Location Verification and Quality on Demand APIs - [View API Descriptions](#)

Business Problem

To support demanding digital applications, such as computer vision and process automation, manufacturers require highly reliable connectivity. If these applications suffer from resource competition and bottlenecks, mission-critical processes can be disrupted.

Impact

The demonstration illustrated how network APIs can significantly improve efficiency and performance in manufacturing environments. The technology could improve productivity and safety, support flexible manufacturing lines and reduce cabling costs. Orange is now implementing a proof of business in France, Spain, Belgium and Poland.

Technical Solution

At MWC25, Orange and Shabodi demonstrated how CAMARA-based APIs can help monitor conditions in factories. When a 5G-connected sensor detected an abnormal temperature, the demo used the Location Verification API to determine the location of the nearest 5G-connected camera. The Quality on Demand API was then employed to ensure the camera had the bandwidth it needed to stream live video, enabling remote personnel to assess and address the situation promptly.

Value

By helping to enhance production lines and optimise factory operations, network APIs can support the further automation of manufacturing through digitisation (a concept known as Industry 4.0). The net result should be greater efficiency and productivity, as well as a lower risk of accidents.

"We leveraged Orange's private 5G network to demonstrate how automation is not just about utilising the network as connectivity, but exploiting the intelligence of the network to realise a vision and capabilities of various automation strategies...the partnership with Orange has enabled Shabodi to expose these complex network services as simple APIs."

Harpreet Geeke
Co-Founder & CTO of Shabodi.

EUROPE

Challenge:

Supporting demanding digital applications, such as computer vision and process automation, manufacturers require highly reliable connectivity.

Mission-critical processes can be disrupted if these applications suffer from resource competition & bottlenecks.

Solution:

- Orange & Shabodi collaborated to build a common set of APIs that the Manufacturing industry use to overcome resource competition & bottlenecks:
 - **Location Verification** determine the location of the nearest 5G-connected camera
 - **QoD** ensures the camera has the bandwidth to stream live video, enabling remote personnel to assess & address the situation promptly

Results:

Shabodi: greater efficiency, productivity & lower risk of

GSMA™

Commercial Case Studies

China Unicom Global: Connectivity Insights & QoD – Cross Border eCommerce Platforms (CITIC Telecom & DT)

GSMA Open Gateway **CONNECTING · THE FUTURE** 连接 · 未来

Quality on Demand API Connectivity Insights API

Telcos team up to support international live streaming

Case study for cross border e-commerce using the CAMARA-standardised Quality on Demand and Connectivity Insights APIs - [View API Descriptions](#)

Business Problem	Technical Solution
Since the pandemic, there has been strong demand for live streaming services, relating to cross-border e-commerce, in the Asia-Pacific region. But content creators have primarily had to rely on traditional roaming services or local tourist SIM cards to stream live. These options are not necessarily cost-effective or don't support the low latency and high bandwidth required for live overseas broadcasts.	China Unicom Global has integrated its API platform with CITIC Telecom's DataMall and Deutsche Telekom's Remote Packet Gateway LBO (local breakout) capabilities to deliver RJet – a mobile data solution tailored for overseas streamers and live streaming platforms. RJet utilises the CAMARA-based Connectivity Insights and Quality-on-Demand APIs to analyse the network quality on users' mobile devices and then improve it, as necessary, to deliver stable connectivity.

Impact	Value
China Unicom Global says the RJet solution, which provides customers with a selection of data packages and acceleration options, is targeted at 500,000 e-commerce cross-border streamers and 1.2 million entertainment and travel streamers, which each tend to use multiple phones.	As a prepaid service, the solution is designed to deliver live streamers high quality and stable connectivity, while eliminating concerns about high roaming fees. The solution also allows the customer to use their existing SIM cards, rather than having to purchase temporary SIM cards overseas.

"Through the learning process of Open Gateway API technology, we have discovered the significant potential of Open Gateway API standardisation with the application of 5G network capability. It can be applied to various application environments. Meanwhile, it allows us to integrate creativity and to complete projects in a short time. Our company has full confidence in the Open Gateway ecosystem."

Dickson Ip,
Chief Technology Officer of CITIC Telecom.



CHINA

Challenge:

Strong demand for live streaming services relating to cross-border e-commerce in the APAC region. Content creators rely on traditional roaming services or local tourist SIM cards to stream live. These options not cost-effective or don't support low latency and high bandwidth for live overseas broadcasts.

Solution:

- China Unicom Global integrated its API platform with CITIC Telecom DataMall and DT Remote Packet Gateway LBO (Local BreakOut):
 - **Connectivity Insights** analyse the network quality on user's mobile device
 - **QoD** ensures the appropriate bandwidth and latency needed for the service is provided when required

Results:

CITIC Telecom: Convenience, stable & high-quality connectivity at low cost

Confidential

GSMA™

Commercial Case Studies

China Mobile: QoD – Payment Gateway (Alipay)

The image is a promotional graphic for Alibaba Cloud's Quality on Demand (QoD) API. It features a red background with a hand holding a smartphone displaying the Alipay app. The text 'GSMA Open Gateway' and 'Alibaba Cloud' are visible. The main headline reads 'Alibaba Cloud increases the reliability of mobile payments'. Below this, it states 'Case study for fintechusing the CAMARA-standardised Quality on Demand API - View API Descriptions'. The graphic is divided into three sections: 'Business Problem', 'Technical Solution', and 'Value'. The 'Business Problem' section describes how unstable mobile connections impact Alipay transactions. The 'Technical Solution' section mentions China Mobile's Ability as a Service (AaaS) platform and the CAMARA-based QoD API. The 'Value' section highlights the adoption of the QoD API and ZTE Network Exposure Function, leading to improved network conditions and service quality.

GSMA Open Gateway

Alibaba Cloud

Quality on Demand API

Alibaba Cloud increases the reliability of mobile payments

Case study for fintechusing the CAMARA-standardised Quality on Demand API - [View API Descriptions](#)

Business Problem

Unstable mobile connections impact about 16% of the hundreds of billions of transactions processed annually by Alipay. Alibaba's mobile payment business. Occurring mainly in densely populated areas, such as shopping malls or transport hubs, or in fast-moving environments, such as on trains, these issues can increase transaction latency and reduce success rates.

Impact

Each day, Alipay initiates two million payment transactions, involving hundreds of millions of yuan, using the Quality on Demand API. As a result, Alipay has reduced average payment latency by 57% and lowered the overall failure rate by 90%.

Technical Solution

Through China Mobile's Ability as a Service (AaaS) platform, Alipay is utilizing the operator's CAMARA-based Quality on Demand API, which provides a programmable interface for developers to request stable latency or prioritised throughput. The API also supports differentiated billing.

Value

China Mobile's QoD API and ZTE Network Exposure Function have been widely adopted to support mobile gaming and mobile payments, with 25 enterprise customers signed up as of Oct 2024. Each month, it processes more than 34 million API calls and has generated tens of millions of yuan in revenue since launch. Users of China Mobile's own Cloud Drive service have experienced a 43% increase in average download speeds and a 22% increase in upload speeds.

"Alibaba Cloud utilises the Quality on Demand API for real-time network quality assurance, ensuring stable and secure network conditions for financial transactions in weak network areas. This integration improves user authentication, network reliability, and overall service quality, addressing challenges of congestion and weak signals in high-traffic areas."

Alibaba Cloud



CHINA

Challenge:

Unstable mobile connections impact about 16% of 100's of billions of transaction processed annually by Alipay (Alibaba's mobile payment). Usually happens in densely populated areas (ex. Shopping malls, transport hubs or fast moving environments like trains) where transaction latency is increased which in-turn reduces success rates.

Solution:

- China Mobile's Ability as a Service (AaaS) platform from ZTE, Alipay is utilizing :
 - **QoD API** – provides programmable interface for developers to request stable latency or prioritized throughput. This API also supports differentiated billing.

Results:

Alibaba Cloud: Improves user authentication, network reliability and overall service quality, addressing challenges of congestion

Confidential

GSMA™

Commercial Case Studies

Telefonica, Vodafone, MasOrange, Laude: Device Locations, QoD, Number Verification, eKYC, SIM Swap – Safety Alert



GSMA Open Gateway

LAUDE

Device Location Verification API

ViRe helps to enforce restraining orders

Case study for personal safety using the CAMARA-standardised Device Location Verification API – [View API Descriptions](#)

Business Problem Restraining orders imposed by the legal system can be difficult and expensive to enforce. Yet, for their peace of mind and personal safety, victims of harassment or assault need to know that the aggressor is complying with such orders.	Technical Solution Developed by i2CAT, Telefónica, Vodafone, MásOrange and LAUDE, the ViRe (Violence Restriction) application employs CAMARA-based APIs to establish a security zone around the victim and their family and frequently visited locations. The solution uses AI to analyse data generated by Device Location Verification, Quality on Demand, Number Verification, Know Your Customer or Device Swap APIs.
Impact ViRe is designed to complement and back up existing protective devices, such as electronic bracelets. In addition, ViRe offers insights into the aggressor's behaviour patterns to help prevent future incidents.	Value The solution strengthens victim protection by ensuring reliable alerts even during periods of network congestion, while reducing costs and intervention times. It represents a robust backup to prevent risk and fraud in restraining orders.

"This model opens up new opportunities for companies like LAUDE to devise innovative applications with a great social impact by taking advantage of the network's advanced capabilities. This new paradigm will allow us to offer new and better services to citizens."

Ana Moliner
Director of the Innovation Business Development Department
& Strategy at i2CAT.



SPAIN

Challenge:

Restraining orders imposed by the legal system can be difficult and expensive to enforce. Yet, for their peace of mind and personal safety, victims of harassment or assault need to know that the aggressor is complying with such orders.

Solution:

- Telefonica, Vodafone, MasOrange & Laude with i2CAT developed the ViRe (Violence Restriction) app using CAMARA API's and AI:
 - **Number Verify, Device Location, SIM Swap, e-KYC**
 - **QoD** ensures the appropriate bandwidth and latency needed for the service is provided when required

Results:

i2CAT: Reliable alerts during periods of network congestion, reduces costs and intervention times. Robust backup for restraining orders.