GSMA Breakfast Briefing

Networks of Trust: Scam Prevention and Privacy Protection through Innovation

GSMA™

Agenda	Time
Welcome remarks from GSMA	7:30 – 7:40
Welcome remarks by Commissioner Dr., Mr. Moon Han Lee, PIPC	7:40 – 7:50
Scams: The human impact	7:50 – 8:00
An introduction to Open Gateway + API case studies	8:00 – 8:15
Official launch: GSMA Implementation of Smart Data Privacy Laws report	8:15 – 8:20
Intervention and open discussion with all stakeholders	8:20 – 8:45
Closing remarks and end of breakfast briefing	8:45 – 8:50

GSMA™

About the GSMA

GSMA

1987

The GSMA was founded

5.7bn+

unique mobile subscribers by end of 2022

12.5bn+

cellular connections worldwide (including IoT)

220m+

lives impacted through Mobile for Development

2016

The first sector to commit to the UN Sustainable Development Goals

2021

Recognized by the UN as a breakthrough sector in the UN Race to Zero climate campaign

50m+

data points included in GSMA Intelligence's database

600

meetings in the past year across all GSMA Working Groups and sub-groups

1.75bn

mobile money accounts

GSMA Membership:

11,000+

mobile operators & companies in the broader ecosystem

Connecting

15,000

experts through Member Gateway – our online community for members

Over

101,000

attendees worldwide attended MWC and Mobile 360 events in 2022

5.5m

visitors to MobileWorldLive.com

GSMA

Welcome remarks by Commissioner Dr., Mr. Moon Han Lee PIPC

GSMA

Scams: The human impact

The global financial cost of cybercrime (criminal activity that involves a computer, network, or networked device), including fraud, is projected to escalate from **USD 9.22 trillion** in 2024 to **USD 15.63 trillion** by 2029 (Statista[1]).

By the end of 2023, **5.6 billion people** or **69% of the global population,** subscribed to a mobile service and **58% of the world's populatio**n used mobile internet, equating to **4.7 billion users.**
(GSMA Mobile Economy Report, 2024[2]).

In 2023 criminals stole over **USD 1 trillion** from victims.
(Global Anti-Scam Alliance[3]).

71% of global organisations reported experiencing at least one successful email-based phishing attack in 2023.
(Proofpoint's 2023 State of the Phish Report[4]).

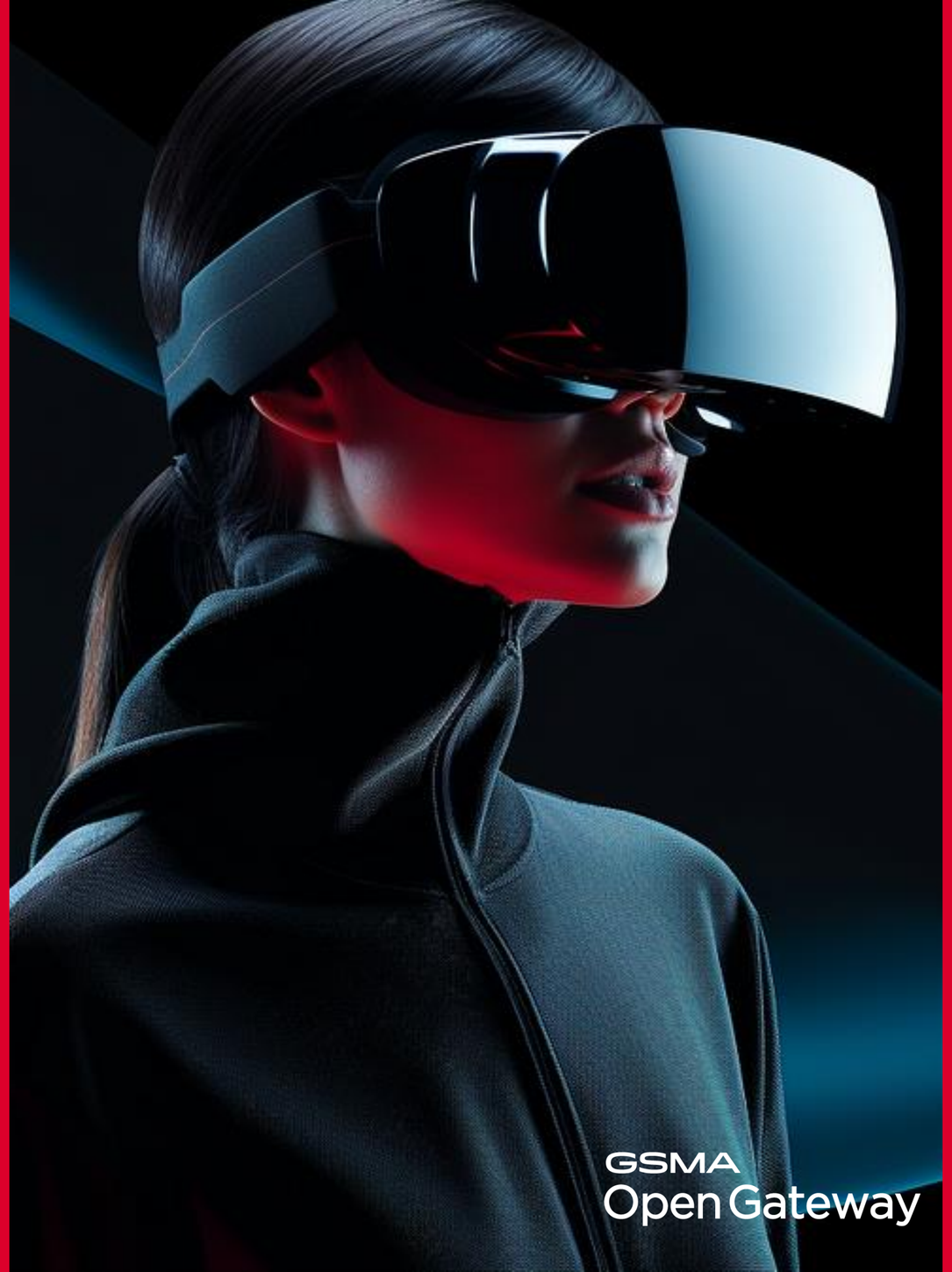
GSMA™

An introduction to Open Gateway + API case studies

GSMA™

GSMA Open Gateway

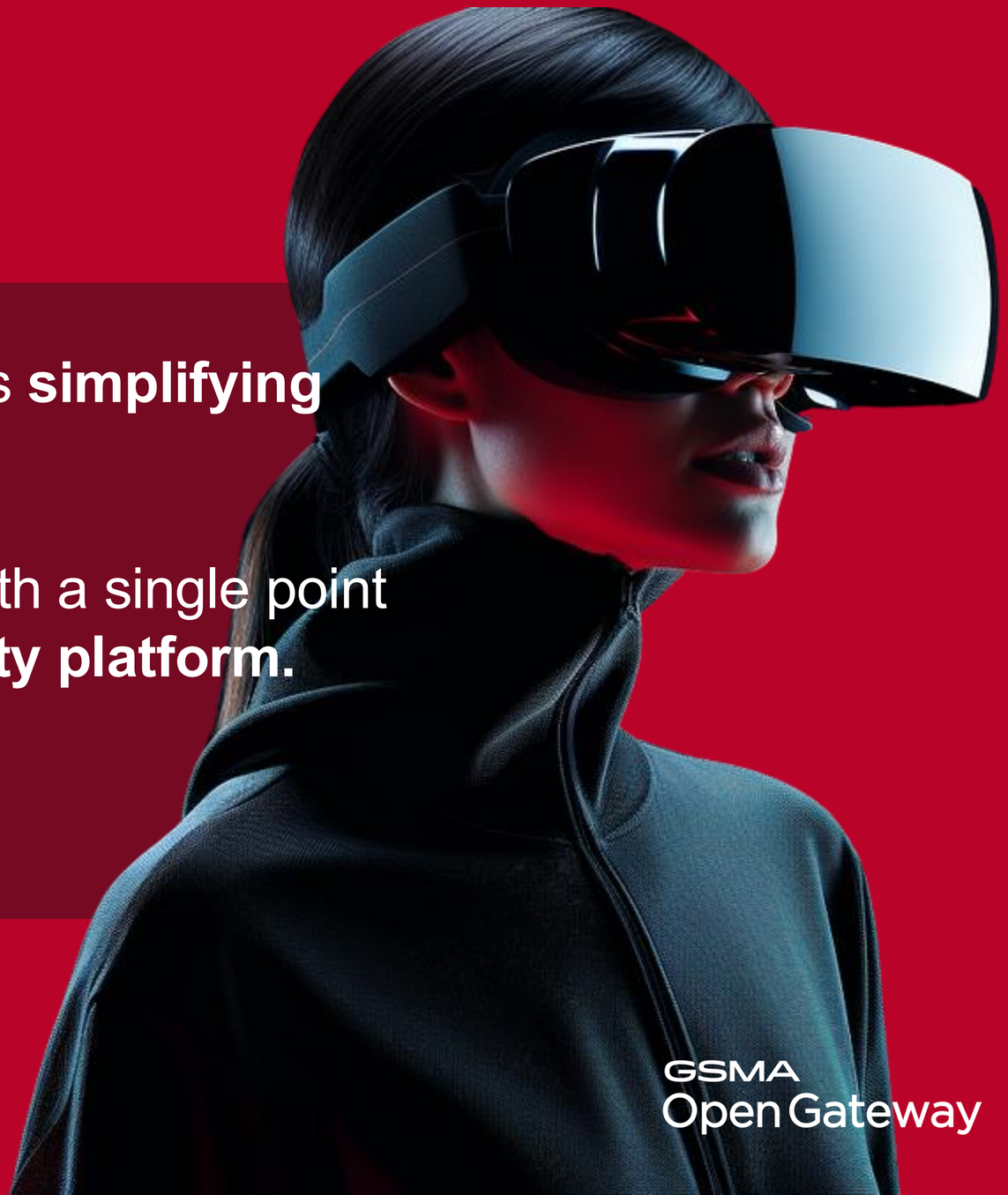
Unleash the power of the network



What is Open Gateway?

A global framework of common network APIs **simplifying access to mobile operator networks**.

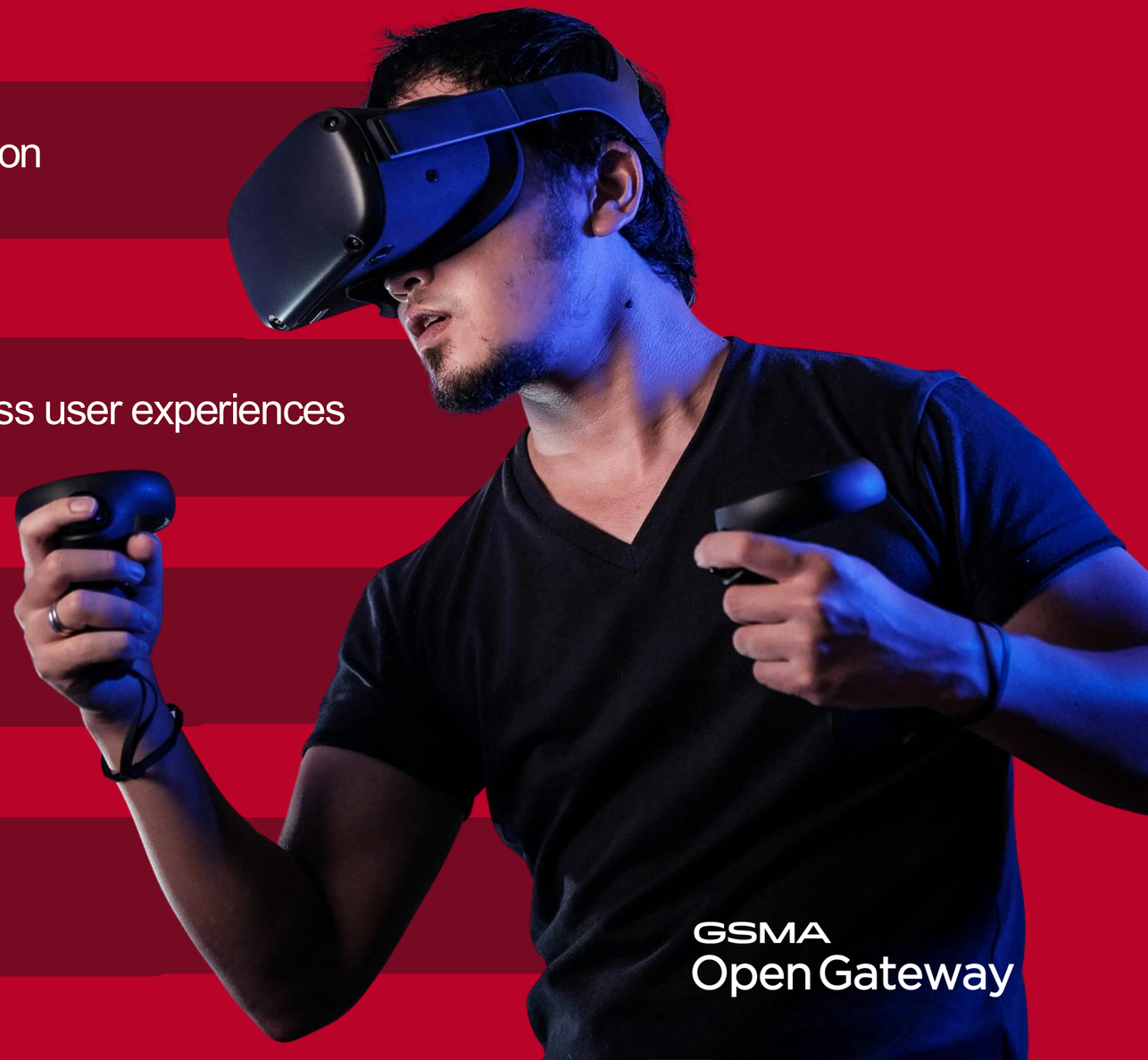
Providing developers and cloud providers with a single point of access to the **world's largest connectivity platform.**



GSMA Open Gateway

Benefits of Open Gateway

- Accelerates service deployment and fosters innovation
- Supports application portability and ensures seamless user experiences
- Helps telecom and tech industries fully realise the potential of 5G
- Standardised open APIs transform how developers build and deliver services



GSMA Open Gateway

API case studies: Vodafone scam signal

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 and value

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.

By addressing a critical need and responding to a 20% increase in fraud, Vodafone and its partners offer comprehensive defences, ensuring legitimate transactions and peace of mind for both end users and banks.

API case studies: Singtel SingVerify

Business problem

According to the Singapore Police Force, there were 50,376 scam cases in 2023 – a 49.6% increase compared to 2022. Phishing scams are among the top five scams, accounting for 12.8% of all scam cases. In total, $651.8 million was lost to scams in 2023. The increase in phishing scams aligns with operators' views on the top security threats facing mobile networks, with phishing and smishing ranked as the most significant threats.

Technical solution

To curb rising scams, Singtel launched SingVerify, offering a suite of tools to authenticate digital identities registered on consumer platforms against mobile operator data.

Built in line with the GSMA Open Gateway framework, the first API under SingVerify is Number Verify, which validates customer identities by matching phone numbers with registered account details.

Impact and value

SingVerify provides **stronger identity verification** via GSMA's Number Verification API., reduces **impersonation fraud** and phishing risks, enhances **user trust and onboarding efficiency** for financial services (Tiger Brokers, IPification), positions Singtel as a **security enabler**, not just a connectivity provider., it creates scalable value through **standardised APIs**, with expansion into Device Location for multi-layer protection.

GSMA

API case studies: Reducing fraud with location data

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.

Technical solution

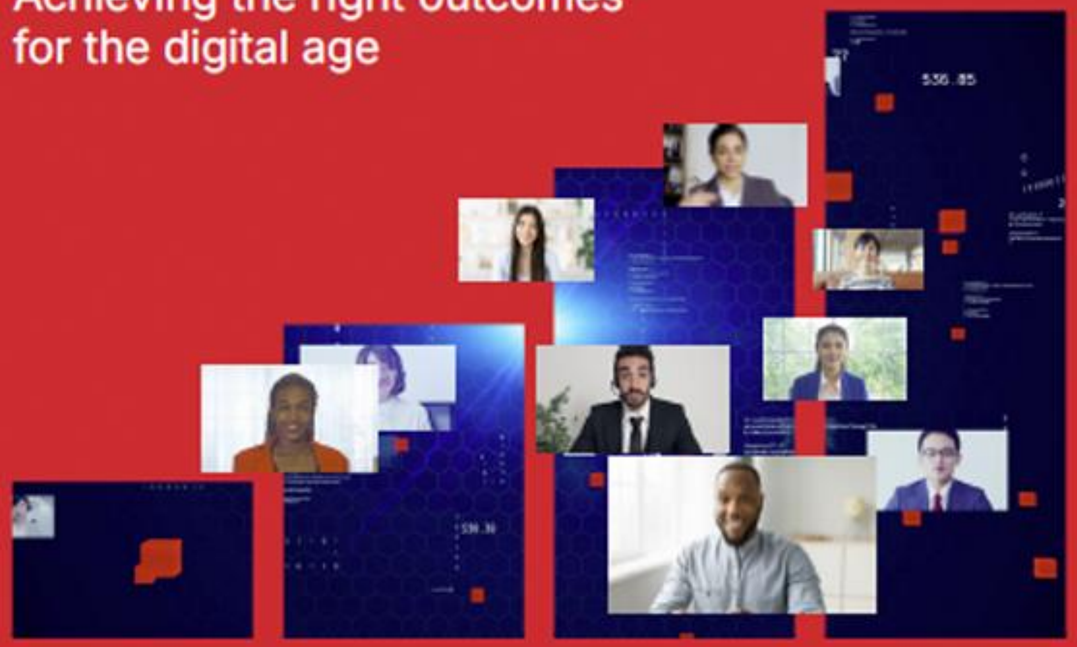
Mobile operators Vivo, Claro and TIM collaborated with Infobip to provide banks with CAMARA-based APIs that can be used to counter scams. Banco Daycoval has integrated the Location Verification API into its application process. The bank now asks applicants whether they consent to sharing their location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

Impact and value

The Location Verification API can reliably verify the geographic position of a device, without the need for GPS, which is vulnerable to spoofing. 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.

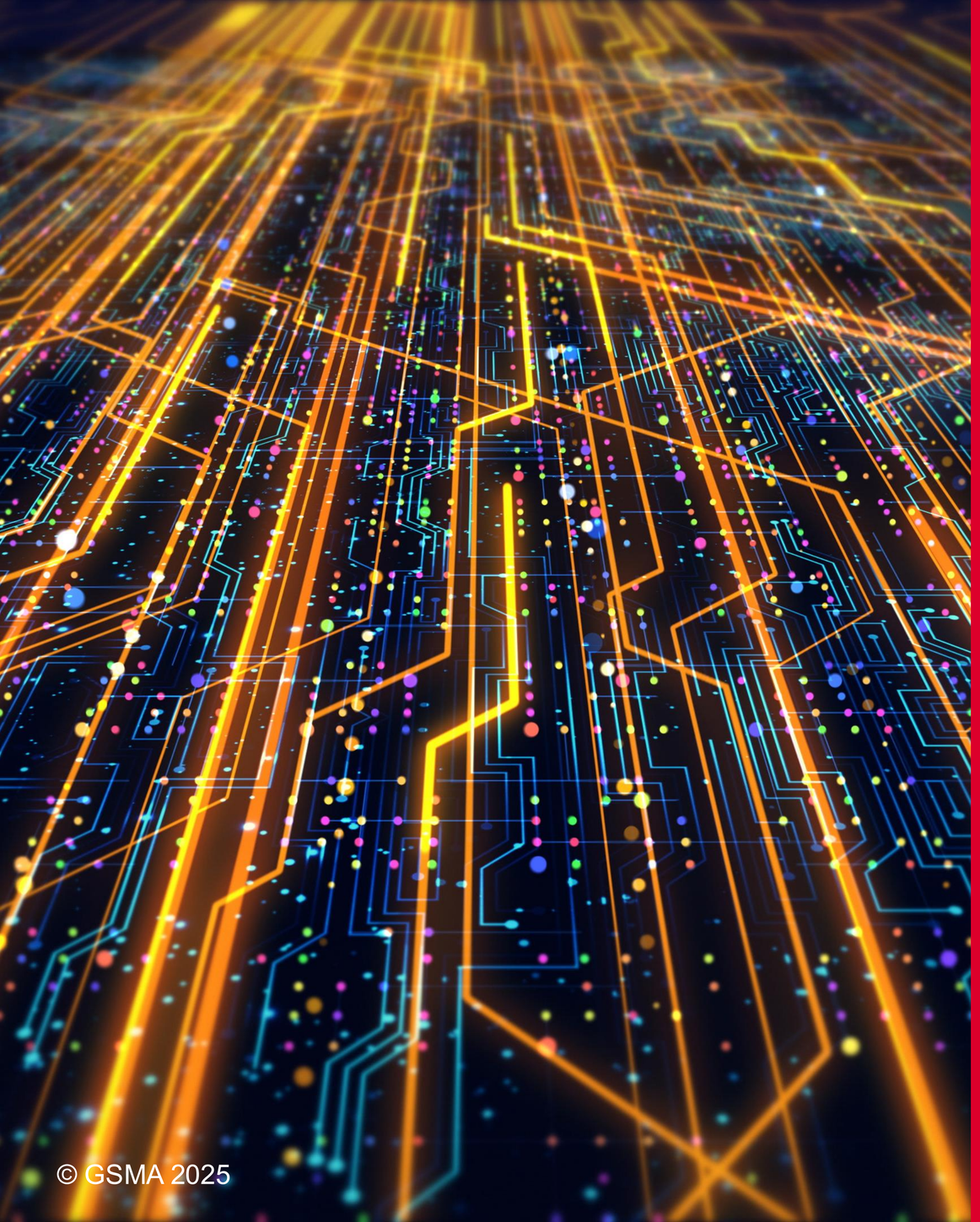
Regulatory sandboxes

Limited regulation	Participants in the sandbox are granted temporary relief from certain regulatory requirements that might otherwise apply to their activities. This allows them to innovate and experiment without being burdened by the full regulatory compliance framework.
Testing ground	Sandboxes serve as a testing ground for new ideas, technologies or financial products. Businesses can validate their concepts and business models without the fear of immediate regulatory consequences if they don't fully comply with existing regulations.
Monitoring & supervision	Regulatory authorities closely monitor the activities within the sandbox to ensure that consumer protection, financial stability, and other critical regulatory objectives are not compromised. This oversight helps strike a balance between innovation and regulatory compliance.
Limited duration	A regulatory sandbox typically has a predetermined time limit, often ranging from several months to a few years. After this period, participants are expected to fully comply with the regular regulatory framework.

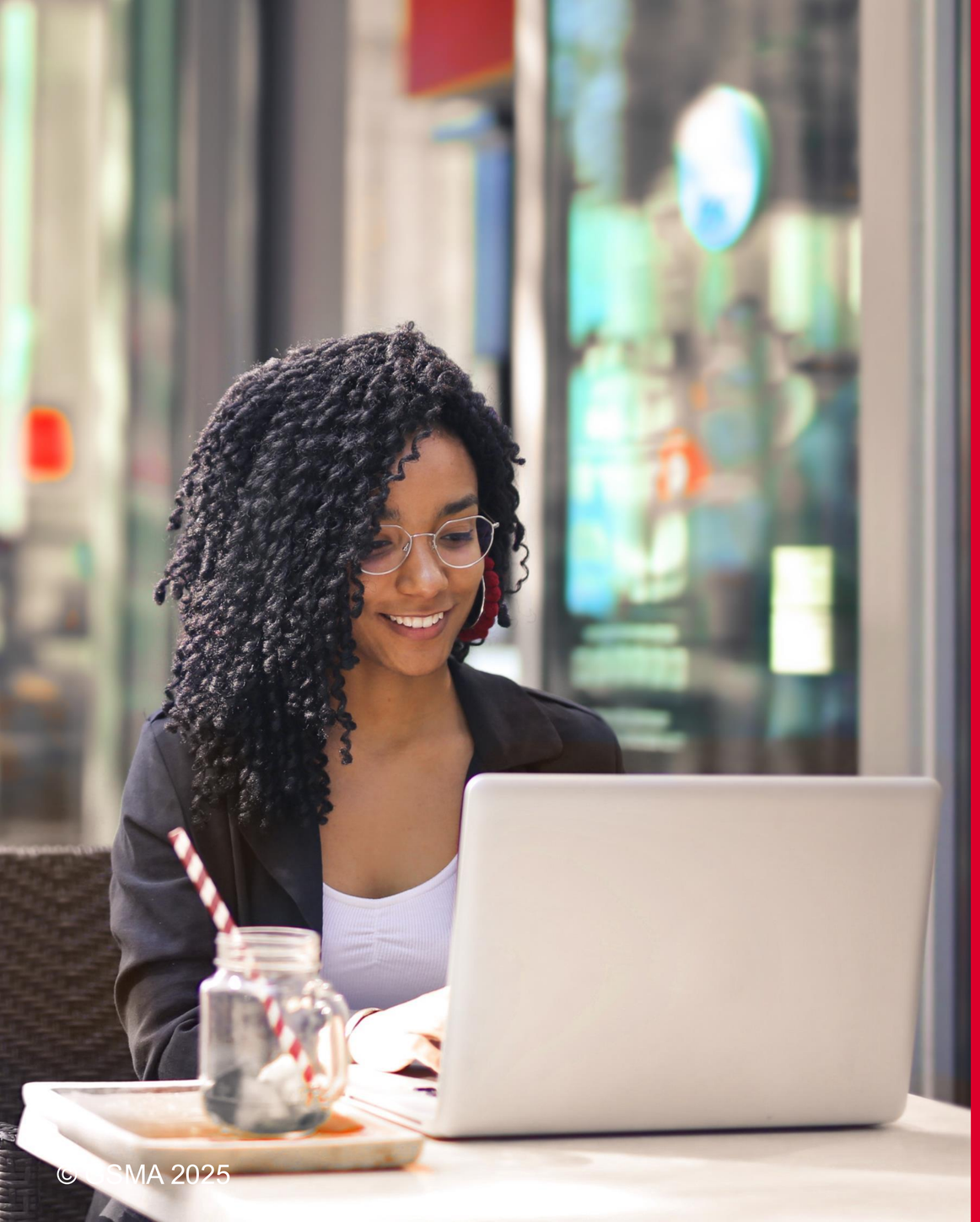


Official launch: implementation of smart data privacy laws report

GSMA™



Intervention and open discussion with all stakeholders



Closing remarks and end of breakfast briefing

Thank you

Download the GSMA App

GSMA