Safe & Secure Mobile Experience:
The Key Issues

Shola Sanni – GSMA Policy Manager, Africa

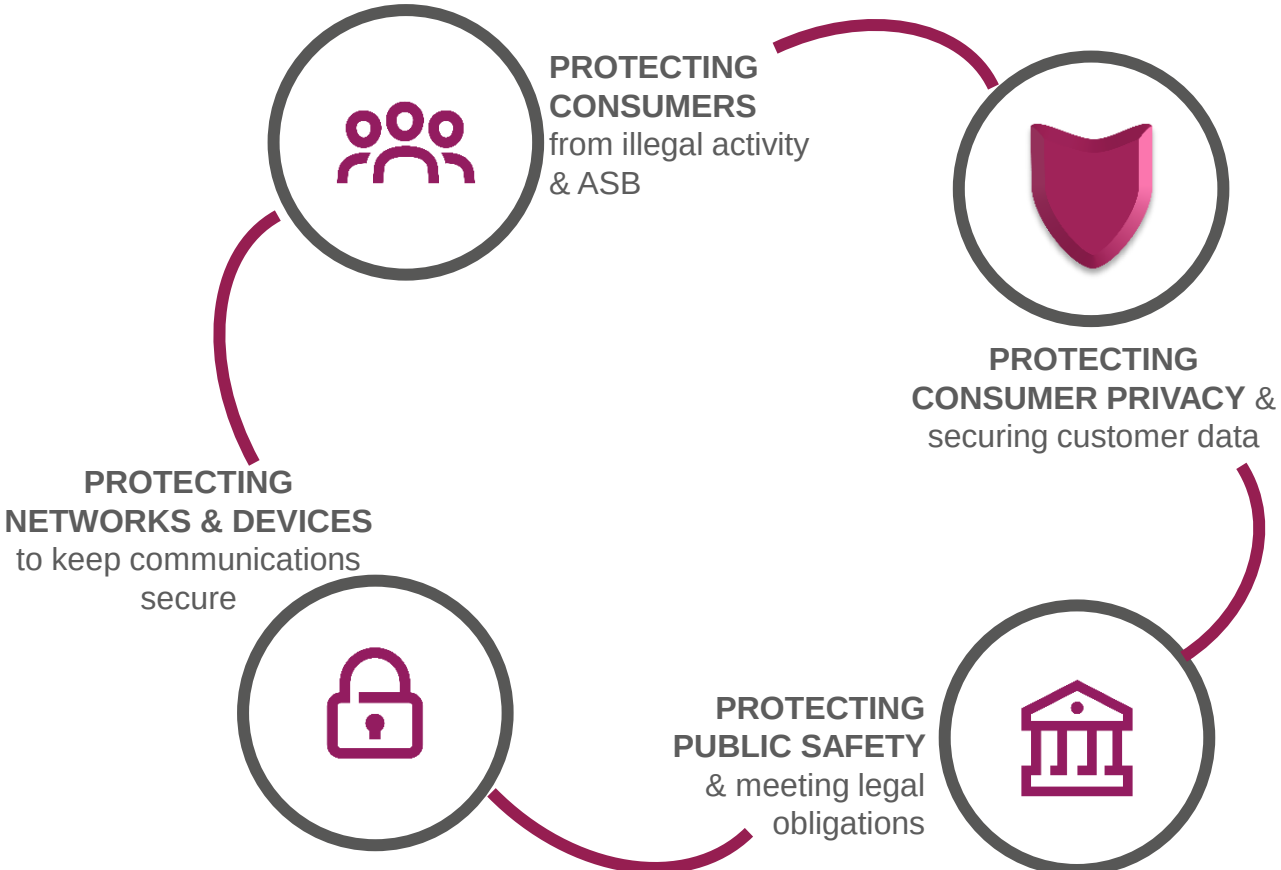
ITU Regional Forum on Consumer Information, Protection & Rights for Africa

Cotonou BENIN, 14-16 March 2017

Outline

- Mobile sector priorities on Safety & Security
- Protecting mobile consumers
- Safeguarding children & vulnerable persons
- Addressing handset theft & counterfeit devices
- Collaboration to combat
- Industry model to combat handset theft
- Fraud via mobile device
- Addressing and minimising fraud
- Bonus slide – Mobile Connect

Mobile sector priorities for Safety & Security



M e sector priorities f afety & Security

Protecting mobile consumers

Key issues in mobile consumer protection

Safeguarding children & vulnerable persons online

Reducing device theft, trade of stolen devices, sale & use of counterfeit devices

Mitigating fraud and mobile device security threats

Safeguarding children & vulnerable persons

Operators

- Prevent access, distribution & promote reporting of online child abuse content – GSMA Mobile Alliance Against Child Sexual Abuse Content
- Encouraging children's safe & responsible internet use – GSMA mYouth program promoting positive use of ICTs
- Supporting inclusion & safety of women through GSMA Connected Women program focusing on security & harassment issues

Government

- Establish clear & transparent legislation regarding illegal content & empower law enforcement before instituting enforcement processes
- Actively collaborate with ecosystem to establish best practices for ensuring online safety & bridging the digital gender gap
- Review policy & regulatory frameworks to promote digital inclusion & avoid undue "blocking" of internet access
- Ensure national reporting hotlines are in place to action online abuse reports

Ecosystem

- Embrace programmes designed to help build "Digital Resilience"
- Educate on potential online issues & encourage positive online behaviours
- Implement technical solutions e.g. parental controls & reporting mechanisms
- Collaborate across ICT ecosystem to address the issues

Addressing handset theft & counterfeit devices

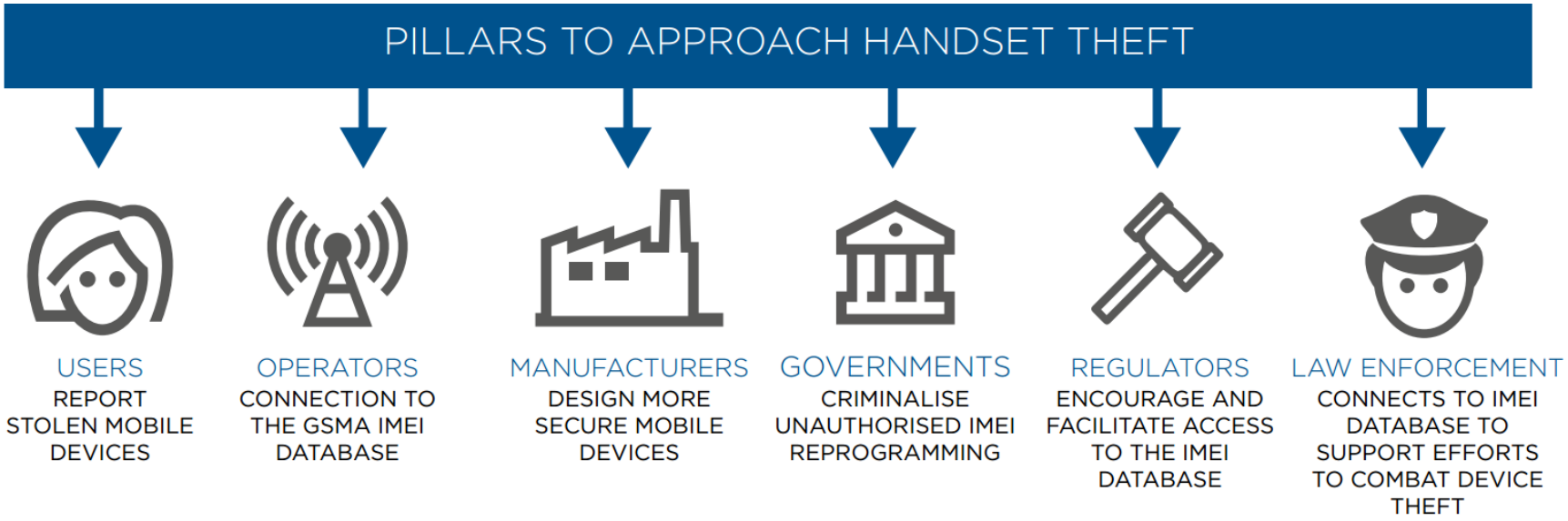
Blacklist – initiative to block stolen mobile devices, based on a shared database of IMEIs of stolen mobile devices reported by consumers

GSMA allocation of IMEIs to 3GPP compliant devices

GSMA Anti-Theft Device Feature Requirements document for implementation of “Kill Switch” capability in devices

GSMA IMEI security initiative - technical design principles for IMEI security implementation & GSMA’s IMEI Security Weakness Reporting and Correction Process

Collaboration to combat



Industry model to combat handset theft

Latin America Case Study

1

HANDSET THEFT FROM USER

Samsung Galaxy

24% 47%

iPhone

are the models which IMEIs are most uploaded to the database

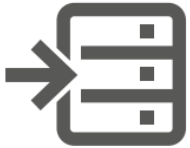
2

USER REPORTS TERMINAL THEFT TO OPERATOR

Units reported daily/per day

Argentina	**5000**
Columbia	**4400**
Brazil	**8200**
Peru	**2800**

3



OPERATOR UPLOADS THE STOLEN HANDSET IMEI TO THE GSMA DATABASE

18 LatAm countries connected to the GSMA database

54 operators in the region (106 worldwide)

+38M uploaded since the commitment signature in July 2012

4

THE REST OF THE OPERATORS IN THE REGION DOWNLOAD THE BLOCKED IMEIS

On average, Latin America operators download data from at least **34 operators of the GSMA database**

5

THE HANDSET STOLEN FROM USER 1 CANNOT BE USED IN OTHER COUNTRIES

Brazil (**6M**) Argentina (**4.1M**) Colombia (**3.2M**) Peru (**2M**)

represents

76%

of all IMEIs from the region uploaded to the GSMA database

Fraud via mobile device

Social engineering fraud : examples

Phishing – method used to infect computers or mobile devices to access valuable personal details – fraudsters use communications like email to tempt people to access what appear to be authentic websites or services

SMiShing – or ‘SMS phishing’ uses phone text messages to deliver the “bait” which then induces people to divulge their personal information

Vishing – when fraudsters persuade victims to hand over personal details or transfer money, over the phone by impersonating a genuine service, e.g. a bank

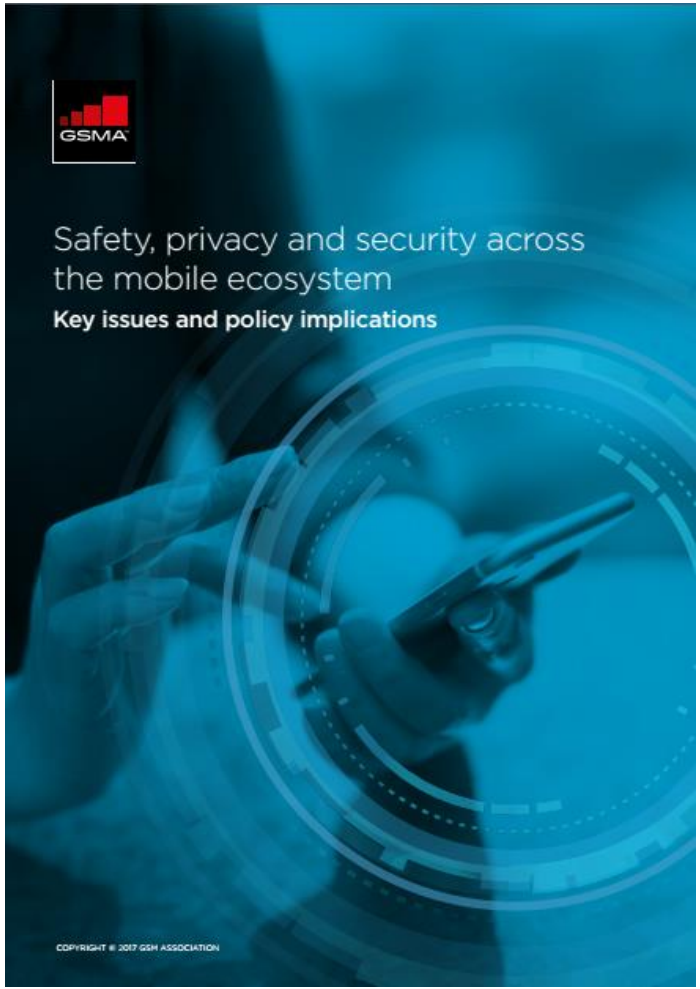
Addressing and minimizing fraud

Role of Operators

- **Technology solutions** – operators adopt GSMA recommended techniques for detecting & dealing with international fraudulent mobile spam
- **Consumer authentication** – Mobile Connect, GSMA guidelines for secure voicemail access
- **Education & awareness** - how to protect personal details and identify potential threats
- Develop robust risk management strategies

Role of Government

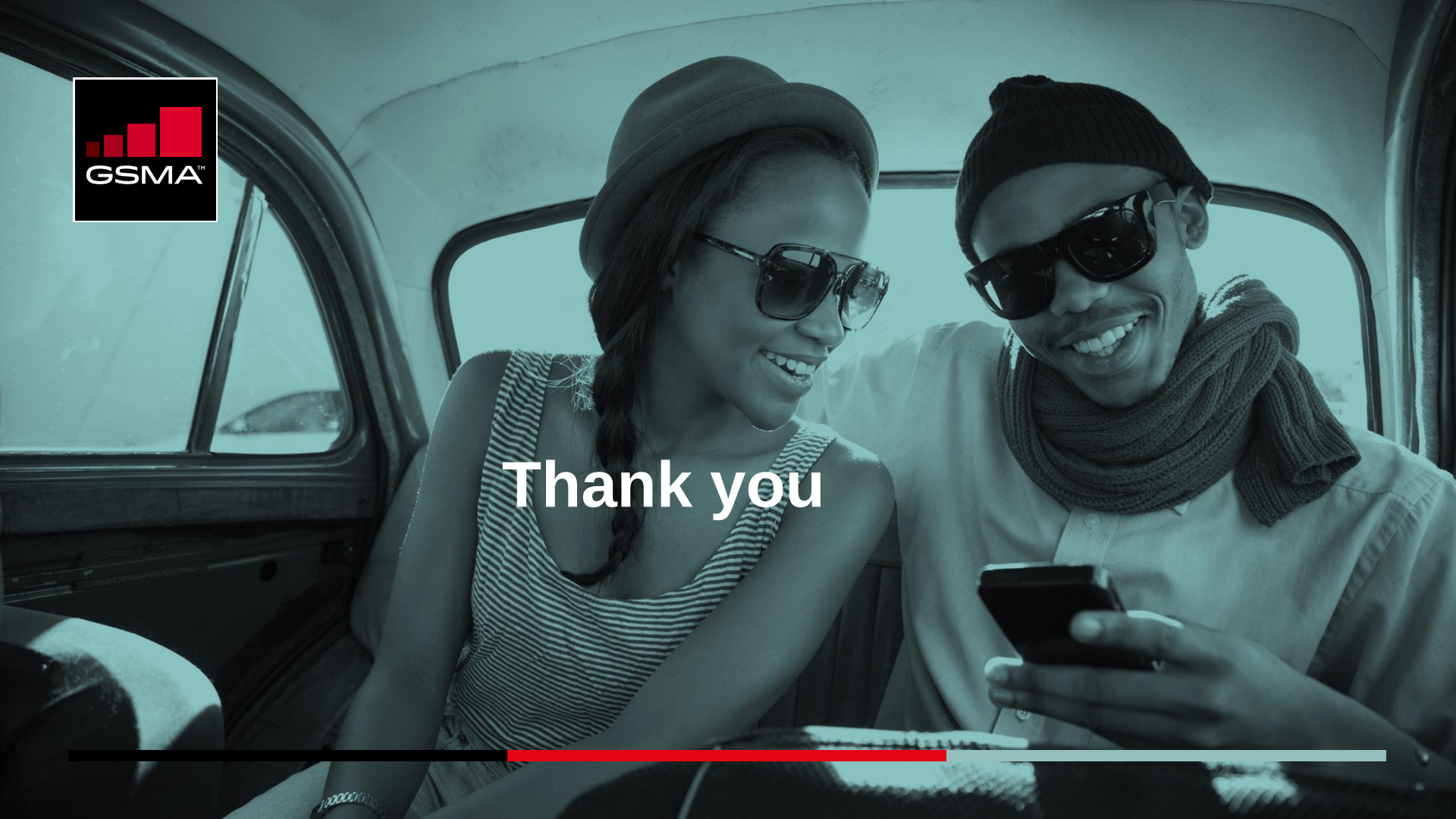
- **Cross-sector enforcement of technology solutions** – ensure banks & retailers implement highest possible level of security measures related to their service
- **Institute legislation and regulation focused on perpetrators**
- **Preventative controls** - consumer awareness campaigns, increase consumer education & protection to help minimise their exposure to fraud



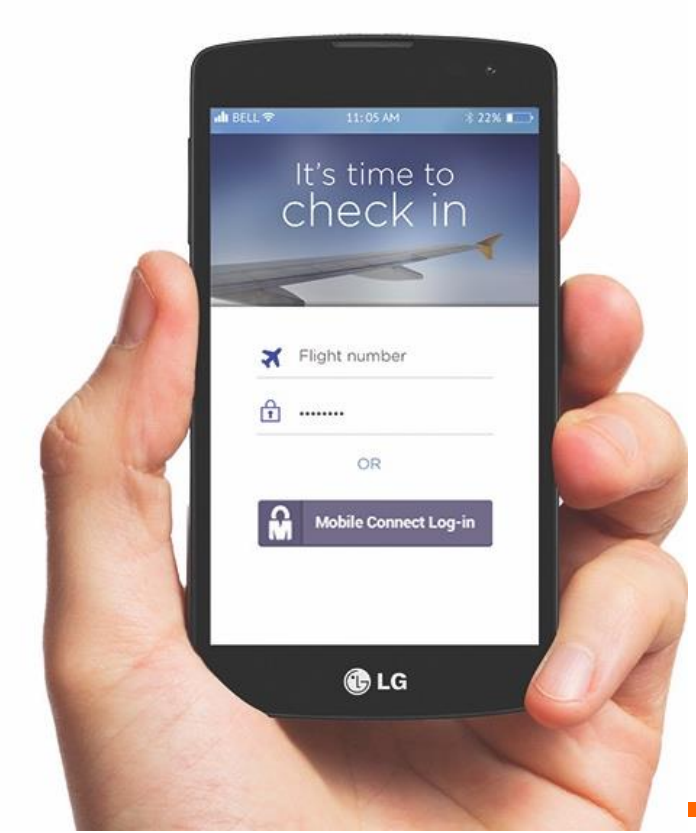
Read more on safety, privacy & security across the mobile ecosystem

Report available at http://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf

Published February 2017


GSMA
Thank you

Mobile Connect – secure and convenient access to digital services



Mobile Connect is a **secure digital identity solution**.

Convenient: easily register and log in to websites and apps, authorising transactions when online, confirming the users' true identity in a secure digital transaction.

With Mobile Connect, no personal information is shared **without the user's permission**: it is convenient, easy to use, and can be trusted to help them be in control of personal data.

88% **of consumers say a single secure login solution would be beneficial**

Sources: GSMA Consumer Research 2015, Cyber Streetwise