Identity Hangout: Monetising Identity Services

5 December 2018

Identity

Monetising

Identity Services

Identity Hangout

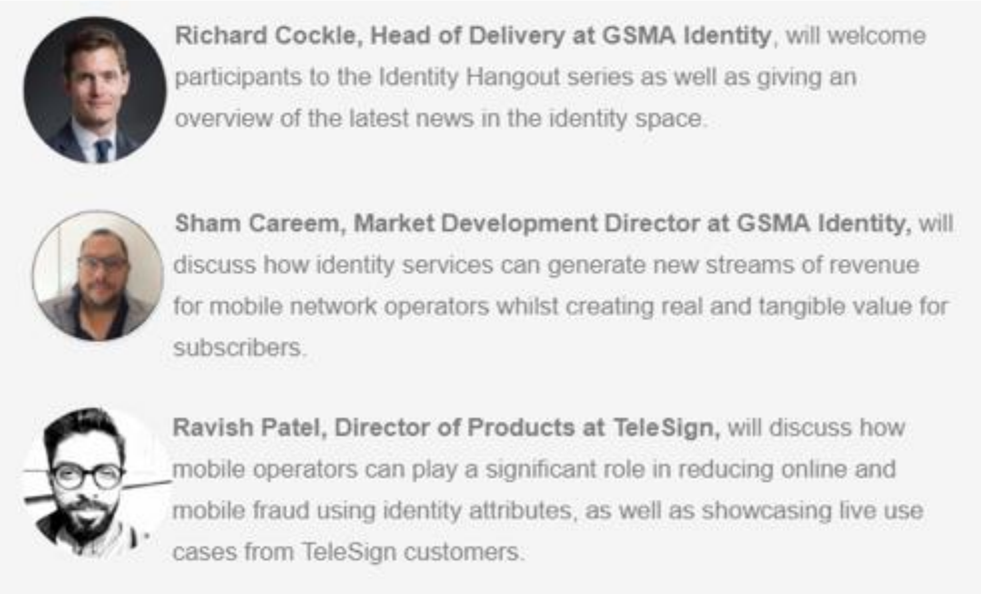
Wednesday, 5 December
15:00 (GMT)

Please dial in +44 203 433 3797 (Meeting ID 571 208) for audio

Mobile Connect Anti-trust note

- Anti-trust law prohibits <u>all agreements</u> (written, verbal, or implicit) between competitors which may negatively impact the market or consumers, *e.g. price agreements, market sharing or exchanging information that can be considered a business secret.*
- Mobile Connect is an authentication, identity and attributes service offered to Service Providers, who are professional corporate buyers in a competitive market of solutions
- To be a feasible solution in the market Mobile Connect requires both technical and commercial level cooperation between mobile operators
- GSMA antitrust assessment has concluded that this cooperation is pro-competitive, on balance, and therefore likely to be permissible under applicable competition law
- Competition law regimes and market conditions differ between countries and regions. Operators are advised to seek local legal advice
- This presentation has been prepared in conjunction with GSMA antitrust policy and its sole purpose is to stimulate thinking and discussion. It does not constitute a GSMA recommendation

Agenda



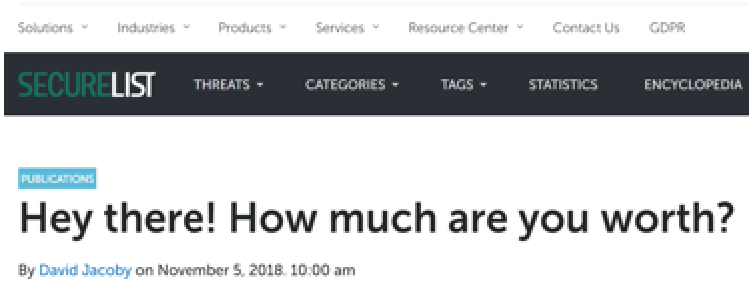
Richard Cockle, Head of Delivery at GSMA Identity, will welcome participants to the Identity Hangout series as well as giving an overview of the latest news in the identity space.

Sham Careem, Market Development Director at GSMA Identity, will discuss how identity services can generate new streams of revenue for mobile network operators whilst creating real and tangible value for subscribers.

Ravish Patel, Director of Products at TeleSign, will discuss how mobile operators can play a significant role in reducing online and mobile fraud using identity attributes, as well as showcasing live use cases from TeleSign customers.

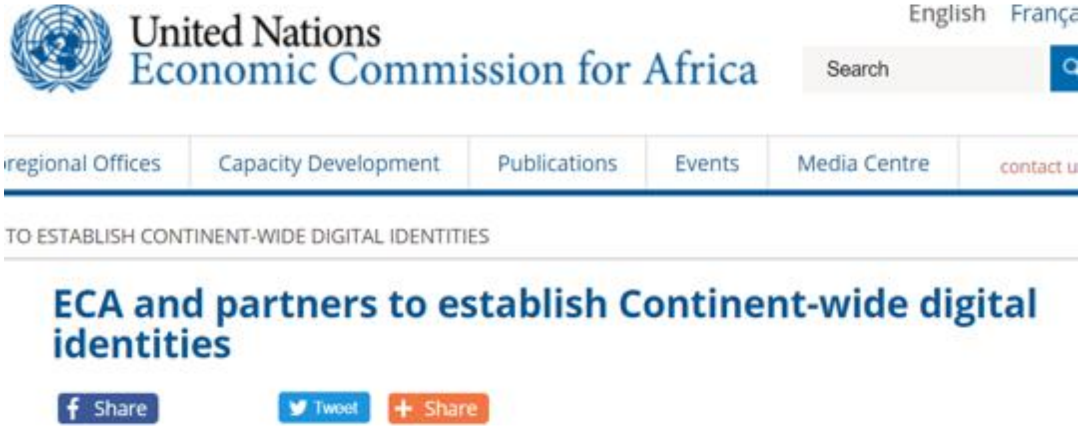
Please dial in +44 203 433 3797 (Meeting ID 571 208) for audio

Identity in the News



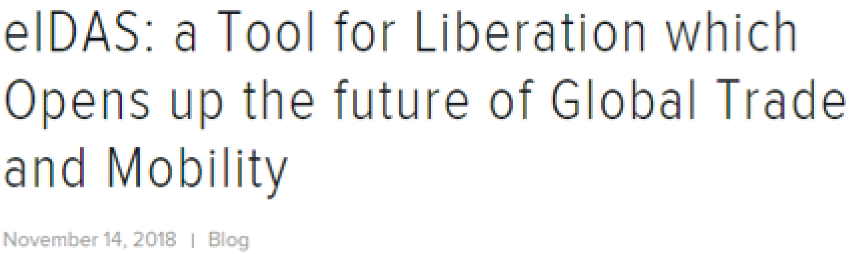
Hey there! How much are you worth?

By David Jacoby on November 5, 2018. 10:00 am



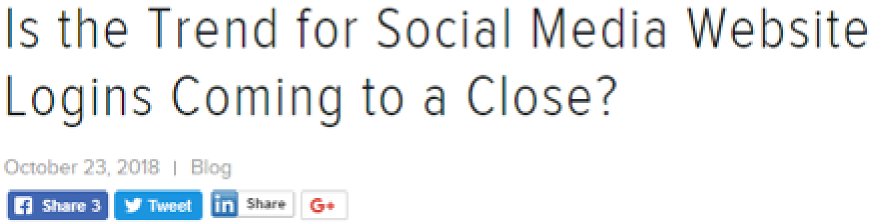
TO ESTABLISH CONTINENT-WIDE DIGITAL IDENTITIES

ECA and partners to establish Continent-wide digital identities



eIDAS: a Tool for Liberation which Opens up the future of Global Trade and Mobility

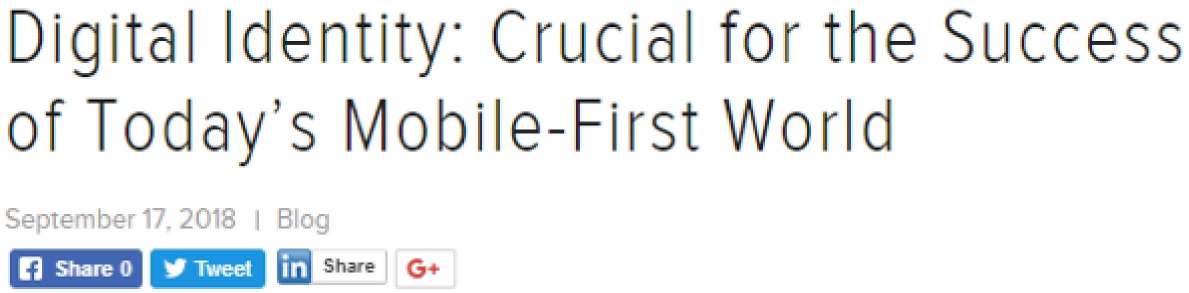
November 14, 2018 | Blog



Is the Trend for Social Media Website Logins Coming to a Close?

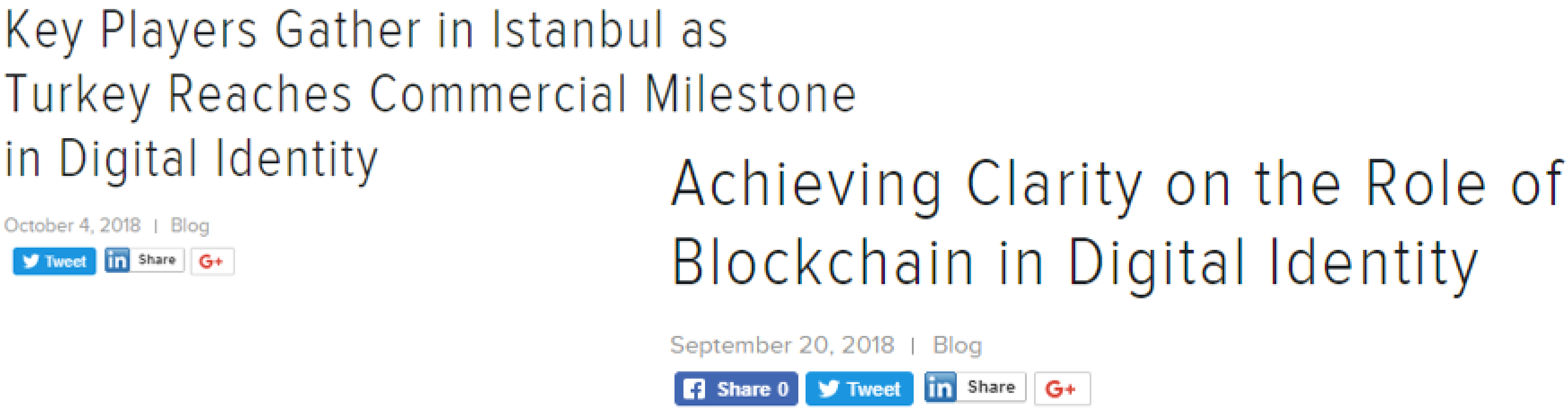
October 23, 2018 | Blog

Identity in the News



Digital Identity: Crucial for the Success of Today's Mobile-First World

September 17, 2018 | Blog



Key Players Gather in Istanbul as Turkey Reaches Commercial Milestone in Digital Identity

October 4, 2018 | Blog

Achieving Clarity on the Role of Blockchain in Digital Identity

September 20, 2018 | Blog

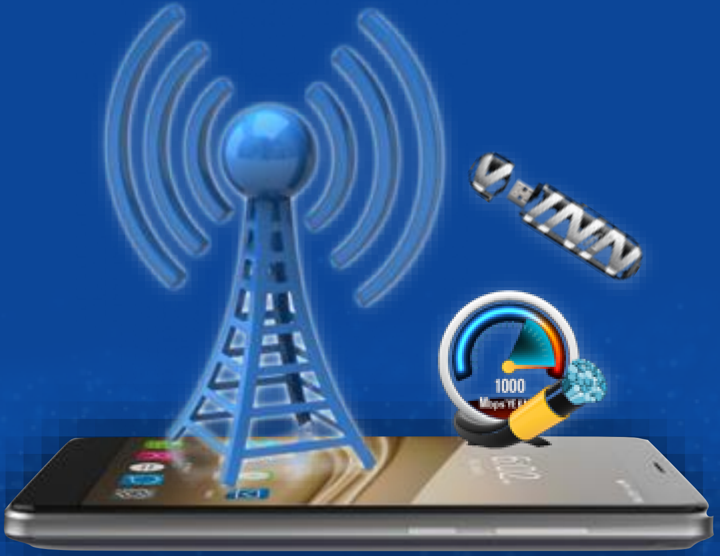
KAAN TERZİOĞLU

Turkcell CEO

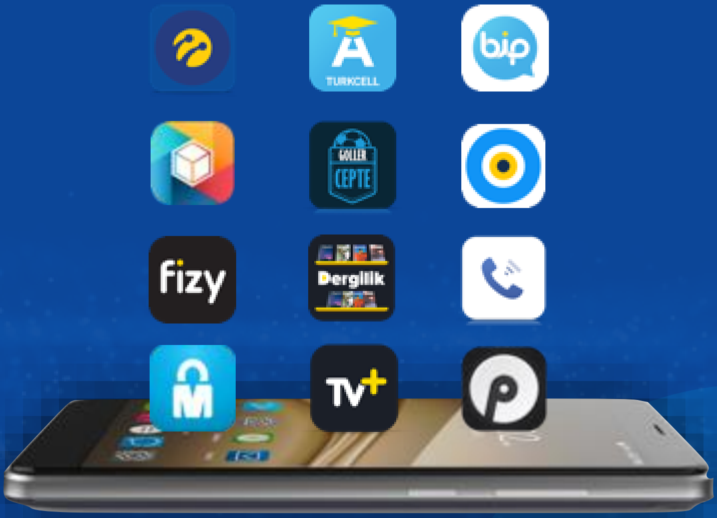
TURKCELL

The Digital Operator

TRANSFORMING INTO THE DIGITAL OPERATOR

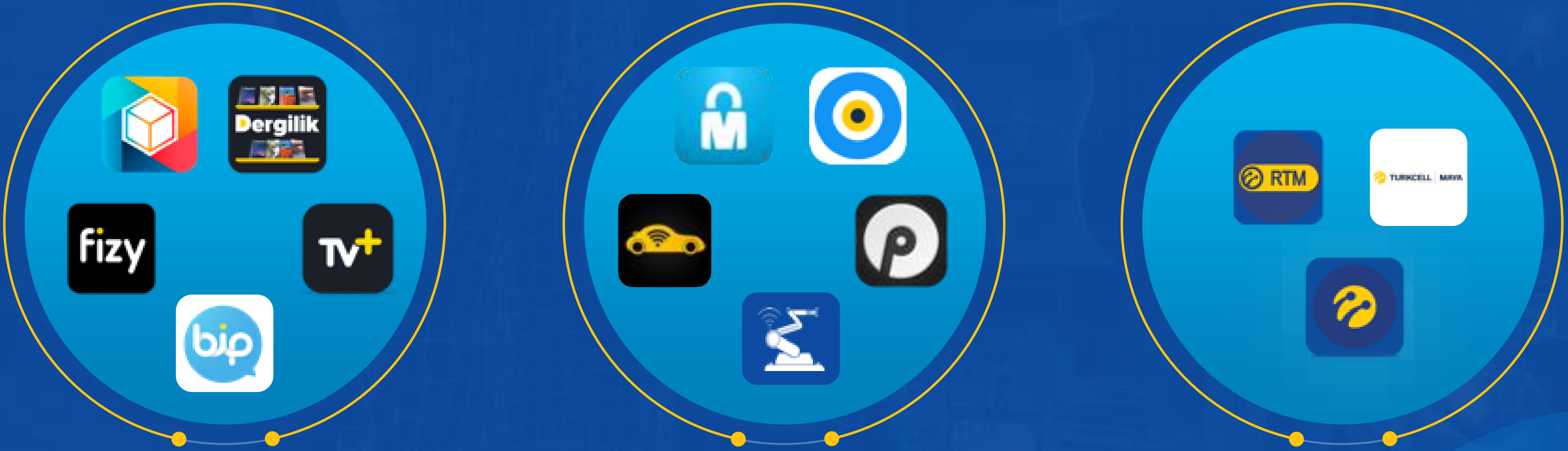


Network Operator



Experience Provider

3 DIMENSIONS OF DIGITAL TRANSFORMATION

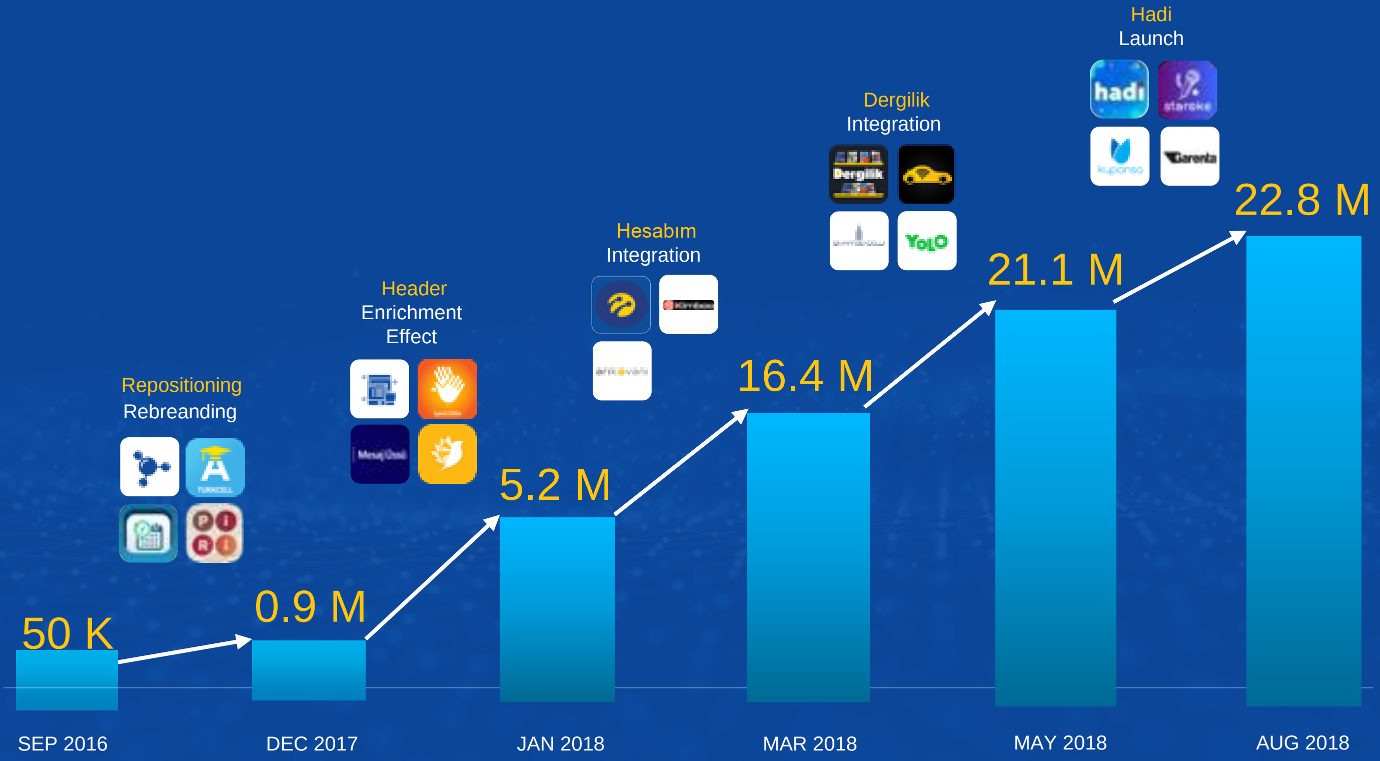


Digital Services

Digital Ecosystem

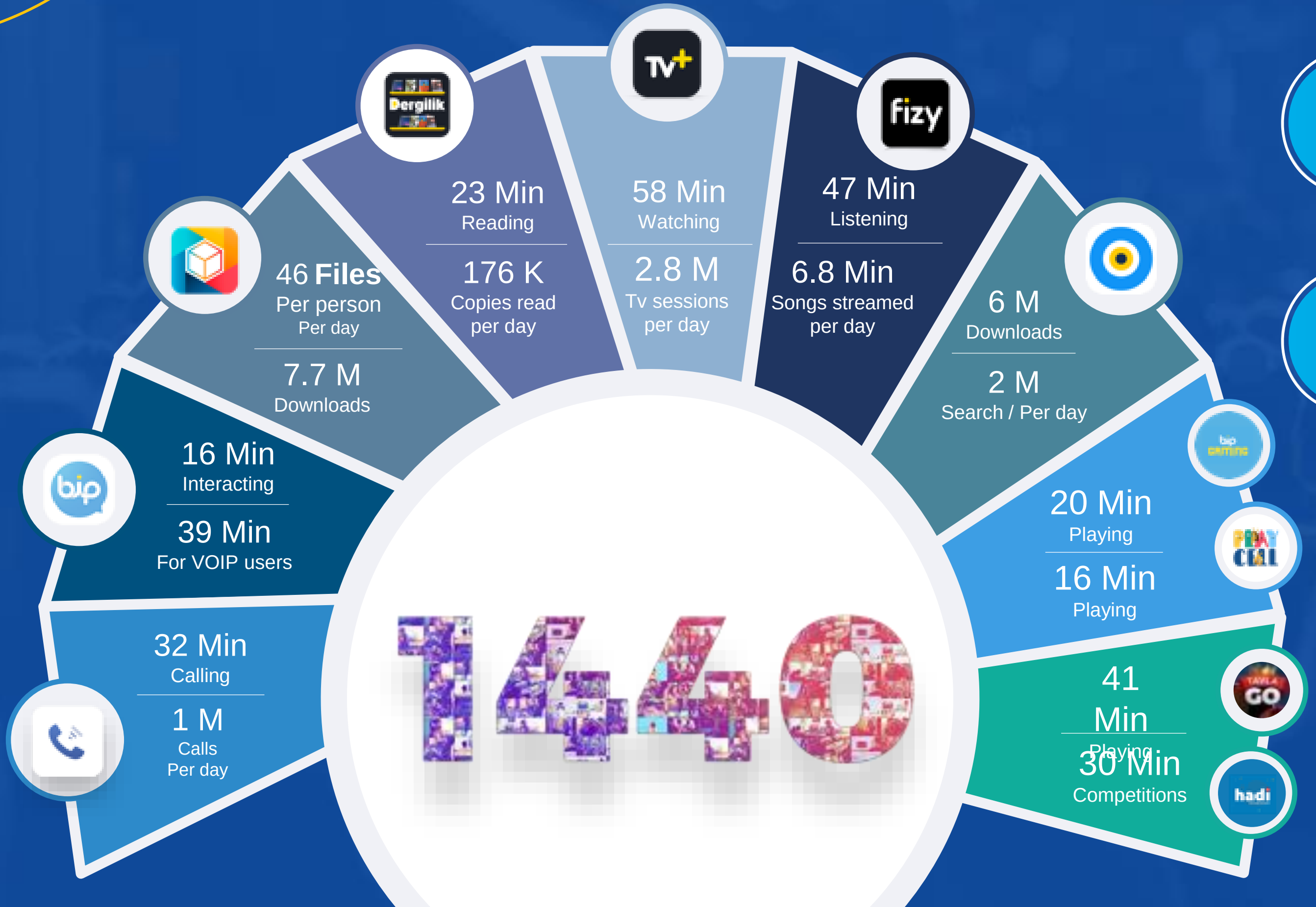
Digital Company

IMPACT OF DIGITAL SERVICES ON MOBILE CONNECT USE



- First Commercially Sustainable Market
- 12 M Registered users
- 31 apps and services integrated
- Accessible to users of all operators

REDEFINING DIGITAL SERVICES



32 Min
Calling

1 M
Calls
Per day

16 Min
Interacting

39 Min
For VOIP users

46 Files
Per person
Per day

7.7 M
Downloads

23 Min
Reading

176 K
Copies read
per day

58 Min
Watching

2.8 M
Tv sessions
per day

47 Min
Listening

6.8 Min
Songs streamed
per day

6 M
Downloads

2 M
Search / Per day

20 Min
Playing

16 Min
Playing

41
Min
Playing
30 Min
Competitions

120 million
core app downloads

- 2nd player in App markets

60.5%
triple-play customers

- Revenue share: 77%
- Lower Churn

DELIVERING VALUE THROUGH DIGITIZATION

52%

Bi-annual growth in Group revenues

107%

Bi-annual growth in EBITDA

42.1%

EBITTA Margin

7 GB

Avarage data use of 4.5G customers in Jun’18

120mn

Core dijital services downloaded

950k

Net add YoY Q2 2018 Turkcell Turkey

Beyond Authentication: Monetising Identity Services

Sham Careem, Market Development Director at GSMA Identity

Can we **monetise** customer data in a user friendly, non intrusive way which adds real **value and utility to our customers?**

Much of the traditional thinking on data monetization has focused on **targeted advertising**

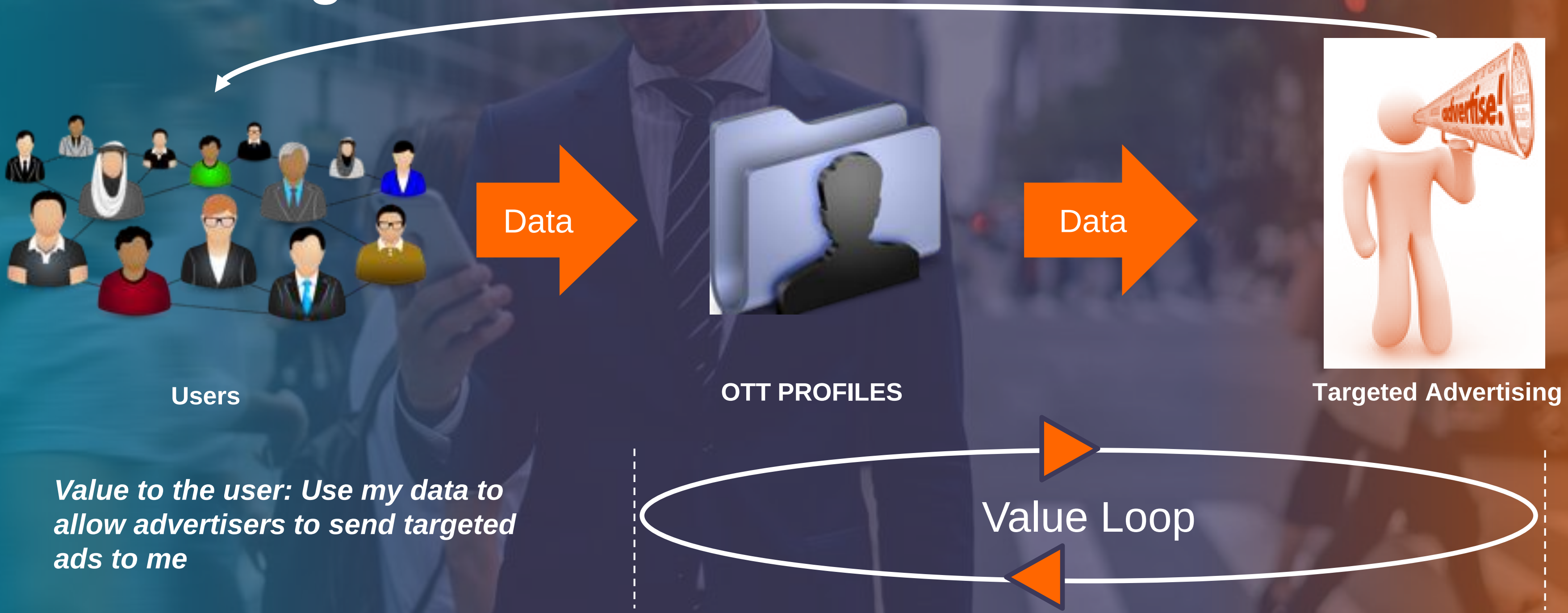
Simple models

Relatively **low investment** needed from MNOs

Generally understood by **consumers**

Trust
Profit
Privacy
Customer Experience

OTT players using user data to create value for advertising networks



Value to the user: Use my data to allow advertisers to send targeted ads to me

Can we **monetise** customer data in a user friendly, non intrusive way which adds real **value** **and** **utility** **to our** **customers?**

Adding value with Mobile Connect

- Fraud Reduction
- New Account Opening
- GDPR Consent Capture
- Payment Authorisation
- Proving Identity
- Password-less Login

What are mobile operator attributes?

Know Your Customer (KYC)

Age

Phone Number

National ID

Account Takeover Protection (ATP)

Location

Lost/Stolen

Network Presence

Account Tenure

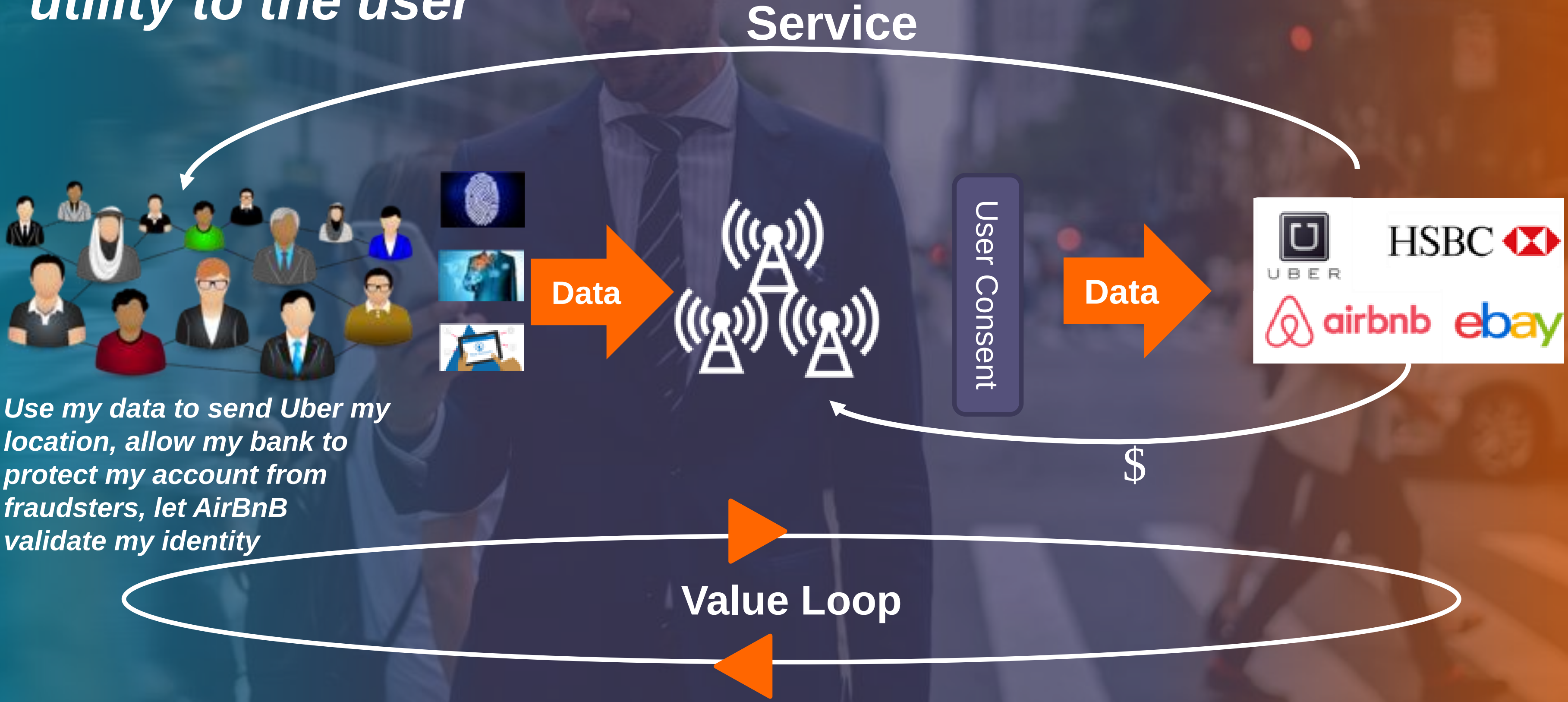
Last Top Up Date

Account type

Billing Segment

Deactivation

MNOs can monetise user data whilst providing *value and utility to the user*



Use my data to send Uber my location, allow my bank to protect my account from fraudsters, let AirBnB validate my identity

End user **consent** is critical to both adherence to regulatory frameworks, and maintaining **end user trust**

- **Informed**
- **Transparent**
- **Stored**
- **Seamless**

Attributes are directly monetisable

Demand

- Organisations transacting with end users are continually looking to improve knowledge of their customers.
  - For better customer experience
  - To increase targeting and cross and upselling
  - To reduce fraud

Supply

- MNOs have a reliable supply of Network and Identity Attributes which meet the demand

Monetisation

- The market has demonstrated clear willingness to pay for these attributes

Attributes market size

$9.3billion

recognised global addressable market size

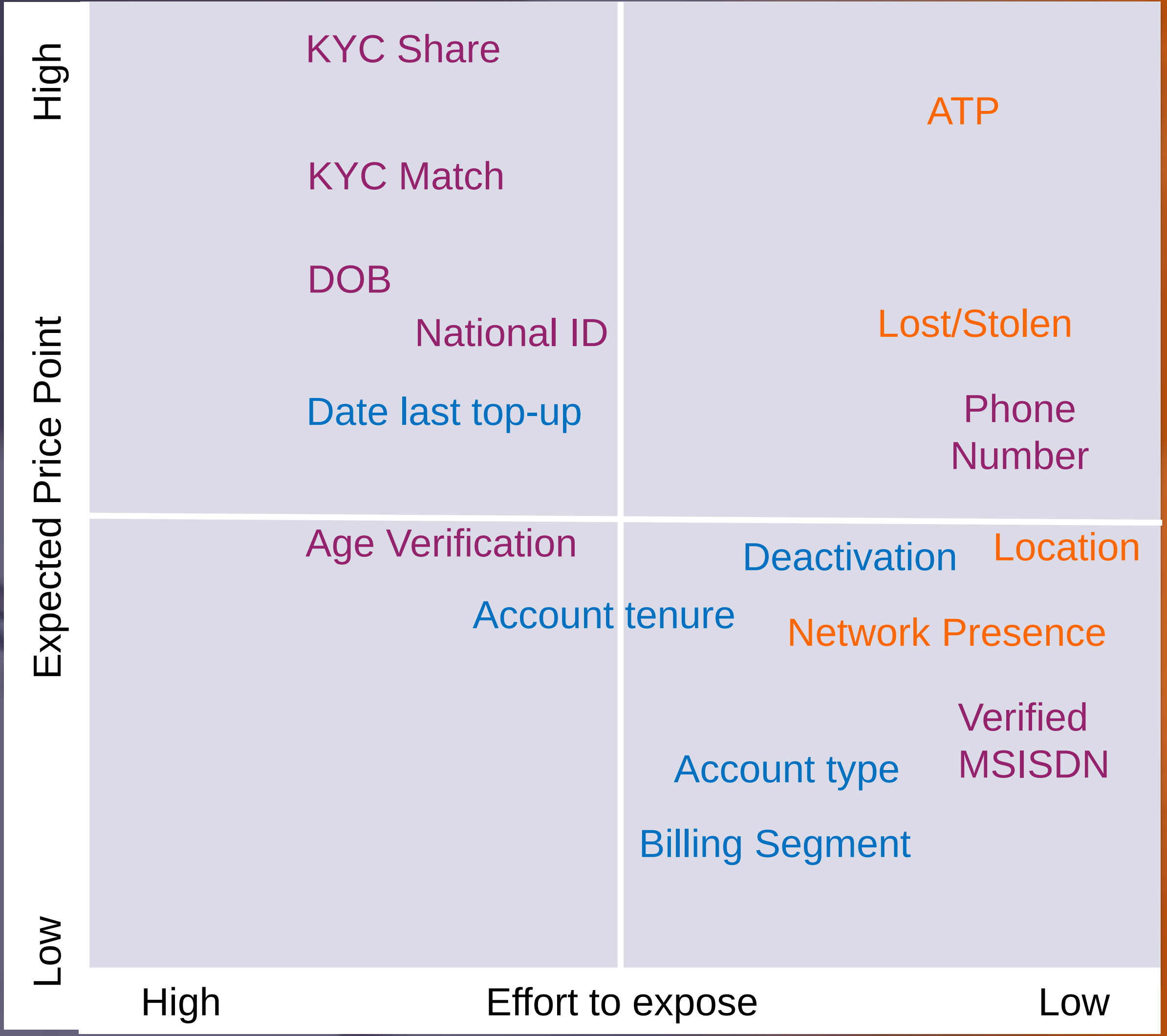
For global Identity and Network attributes in 2020 (USD$):

- Market size estimate will grow as more use cases are recognised as addressable by operators

Identity

Network

Account



Expected Price Point

High

Low

Effort to expose

High

Low

KYC Share

KYC Match

DOB

National ID

Date last top-up

ATP

Lost/Stolen

Phone Number

Age Verification

Account tenure

Deactivation

Location

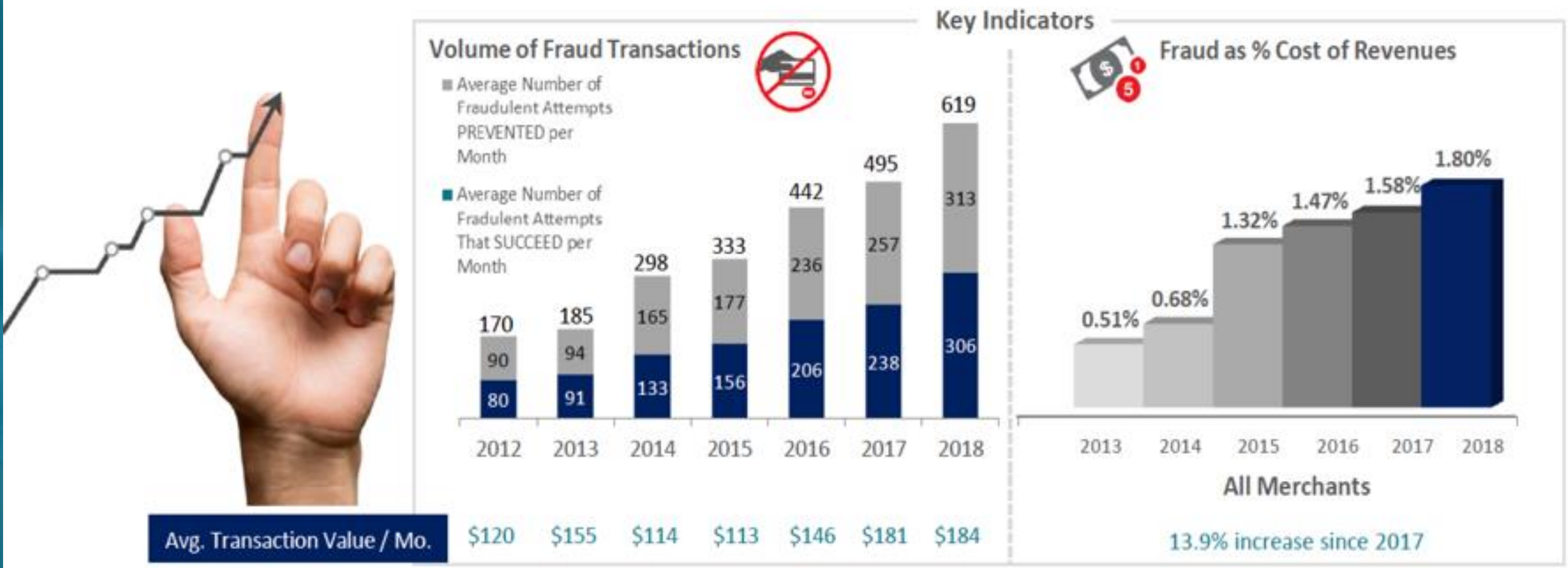
Network Presence

Verified MSISDN

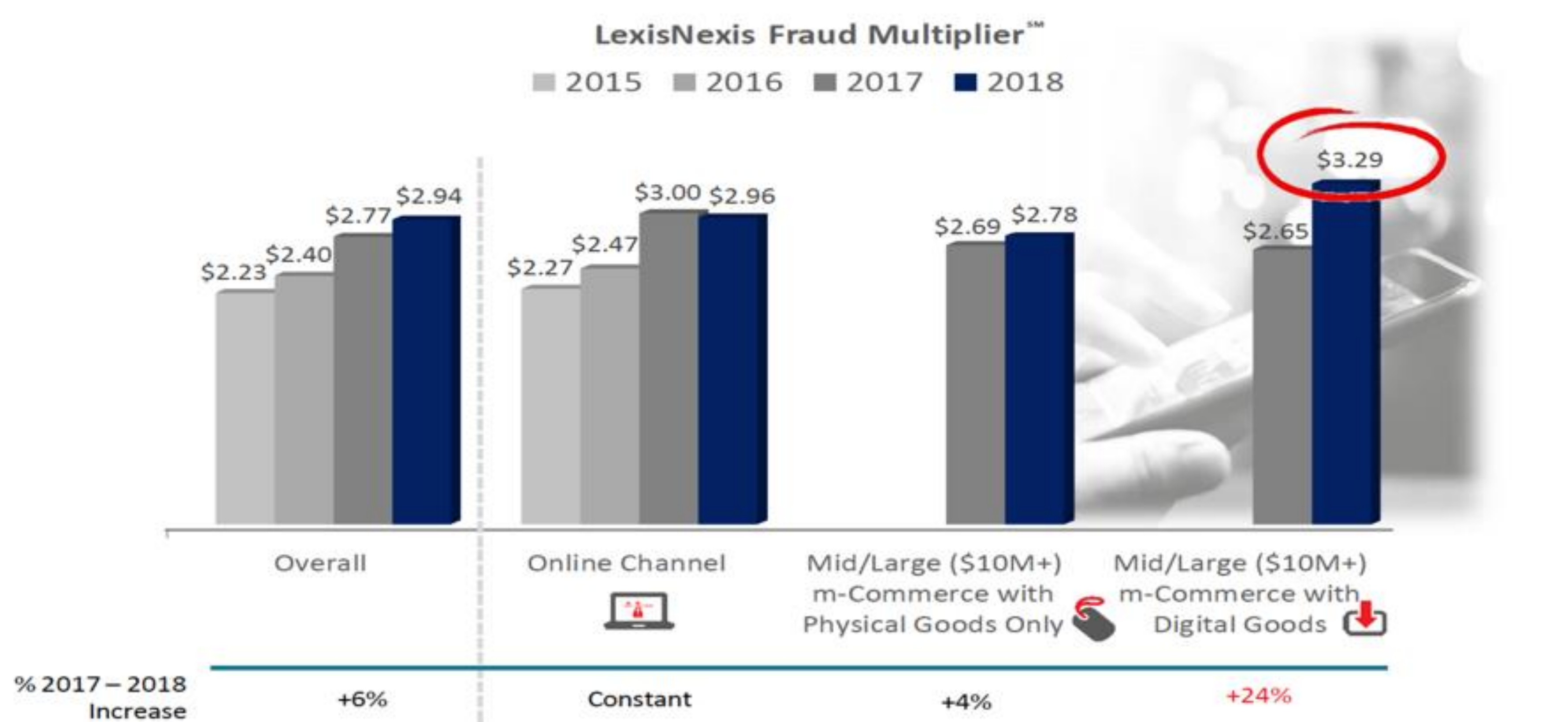
Account type

Billing Segment

Fraud continues to grow



And cost of fraud via the mobile channel is growing fastest



UK Business Snapshot - Banking: KYC and Account Takeover Protection (ATP)

UK Annual Revenue

£30.8million

recognised market size

For KYC and ATP 2020 (GBP£):

Market size estimate will grow as more use cases are recognised as addressable by operators

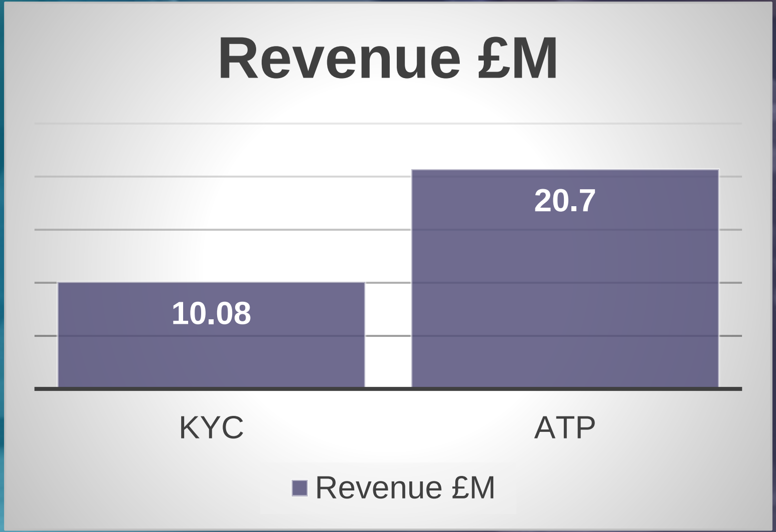
account takeover protection

KYC match

Snapshot Description	**A detailed analysis of the UK banking sector was carried out on a sub set of Mobile Connect attribute products. No other sectors are included in this analysis.**
Product Set	**KYC and ATP**
Methodology	**Based upon a subset of real transactions carried out with UK MNOs and banks**
	Extrapolated to include all banks and MNOs in the UK

UK Business Snapshot - Banking: KYC and Account Takeover Protection (ATP)

Revenue breakdown by Product



Key Assumptions

- 101M UK bank accounts
- 2.5 ATP transactions per year per account
- 1.5 KYC transactions per account per year (including back book check regulatory compliance)
- 60% response rate to KYC request

Are **Mobile Connect attributes** the answer?

WIN WIN

CUSTOMERS

- Derive more value from their mobile operator
- Increase convenience and security

OPERATORS

- Highly profitable new service
- Deeper relationships with customers

TeleSign

Monetizing Identity Services

Ravish Patel

Director – Mobile Identity

Rpatel@Telesign.com

Agenda

1. BICS - TeleSign Introduction
2. Mobile Identity - Commercial Use Cases & Demand
3. Why Mobile Operators should embark on Mobile Identity ?
4. Where should you start ?

TeleSign

TeleSign Introduction

WHO WE ARE

2005

2FA Mobile Identity Pioneer

- *17 Patents Granted*

2010

+Mobile Identity Intelligence

- *Gartner Magic Quadrant Authentication Leader*

2016

+5 Billion Mobile Verification *Transactions globally*

bics + TeleSign

2017 and beyond

+BICS to Acquire TeleSign

- *Expanded data partnerships via BICS*
- *800+ connections to Mobile Operators*
- *BICS owned by Proximus, Swisscom & MTN*

Bridging Digital World with Mobile Operators

Connecting 5000 Digital Services with 800+ MNOs

salesforce EVERNOTE Telegram OLX GROUP HomeAway

Alibaba Group 阿里巴巴集团 meetme anibis.ch Tripster AOL

Banks
Fintech
Cryptocurrency

Rideshare
Marketplaces
Classifieds

Dating
Match
Websites

Gaming
MMORPG

Instant Messaging
& Chat

Social Media
& Networking

bics

Mobile Identity Consulting

- Business Opportunity Validation
- Technology & API Development Consulting
- Privacy & Regulatory Assessments

+

Mobile Identity Monetization

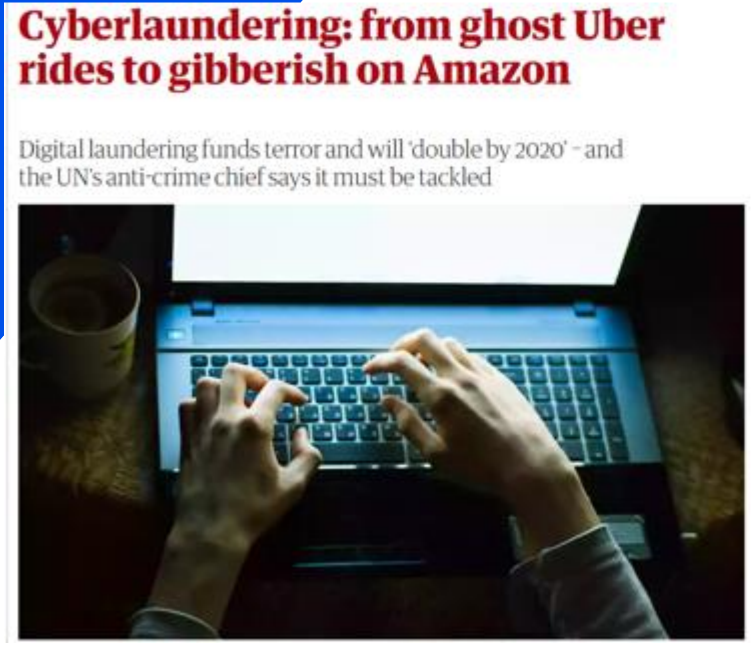
- Mobile Identity Marketplace
- Partnerships with Global Mobile & Web Companies
- New Revenue Generation

TeleSign

Mobile Identity Attributes

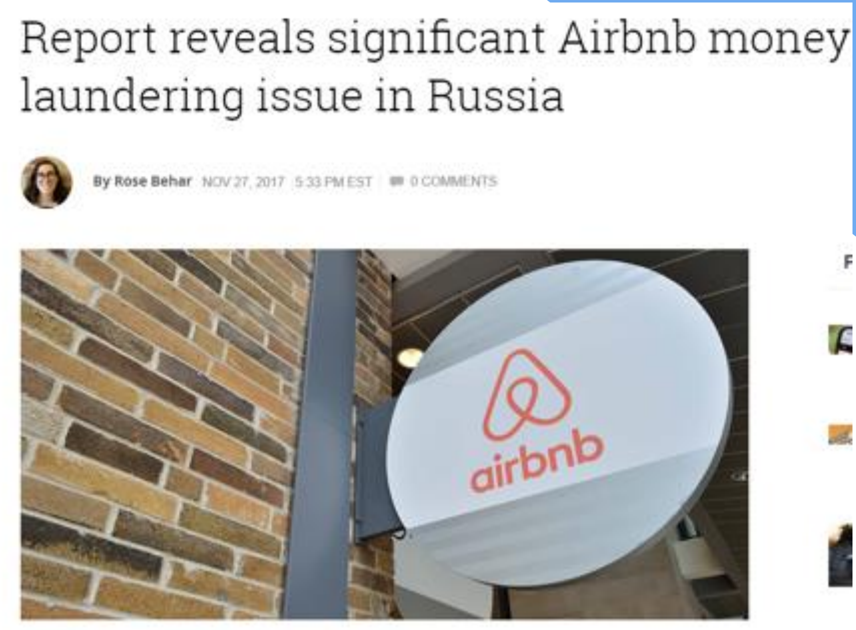
Commercial Use Cases & Demand

Compliance & KYC Risks



Cyberlaundering: from ghost Uber rides to gibberish on Amazon

Digital laundering funds terror and will 'double by 2020' - and the UN's anti-crime chief says it must be tackled



Report reveals significant Airbnb money laundering issue in Russia

By Rose Behar NOV 27, 2017 5:33 PM EST 0 COMMENTS

TeleSign

Data Point: Name/Address Match of Subscriber

DATA POINT

Name and address of the subscriber

- EXAMPLE:
  First Name: John
  Last Name: Doe
  Address: 123 Main St
  City: Los Angeles
  Zip Code: 90007
- Date of Birth – 18 Oct 82

CLIENT TYPES

- Banks/fintech
- Cryptocurrency
- Ecommerce

DEMAND

High

VOLUME

High

ELASTICITY

High

- There are other sources of name/address information available (keyed off email, non-authoritative phone data, etc.)
- If not available, alternative verification types will be used (ID scan, KYC questions, etc.)

STOP FRAUDSTERS FROM CREATING ACCOUNTS

WEBSITES/APPS HAVE HUGE PROBLEMS WITH FAKE ACCOUNTS

Using bots, fraudsters create millions of online, social media, email, and other accounts

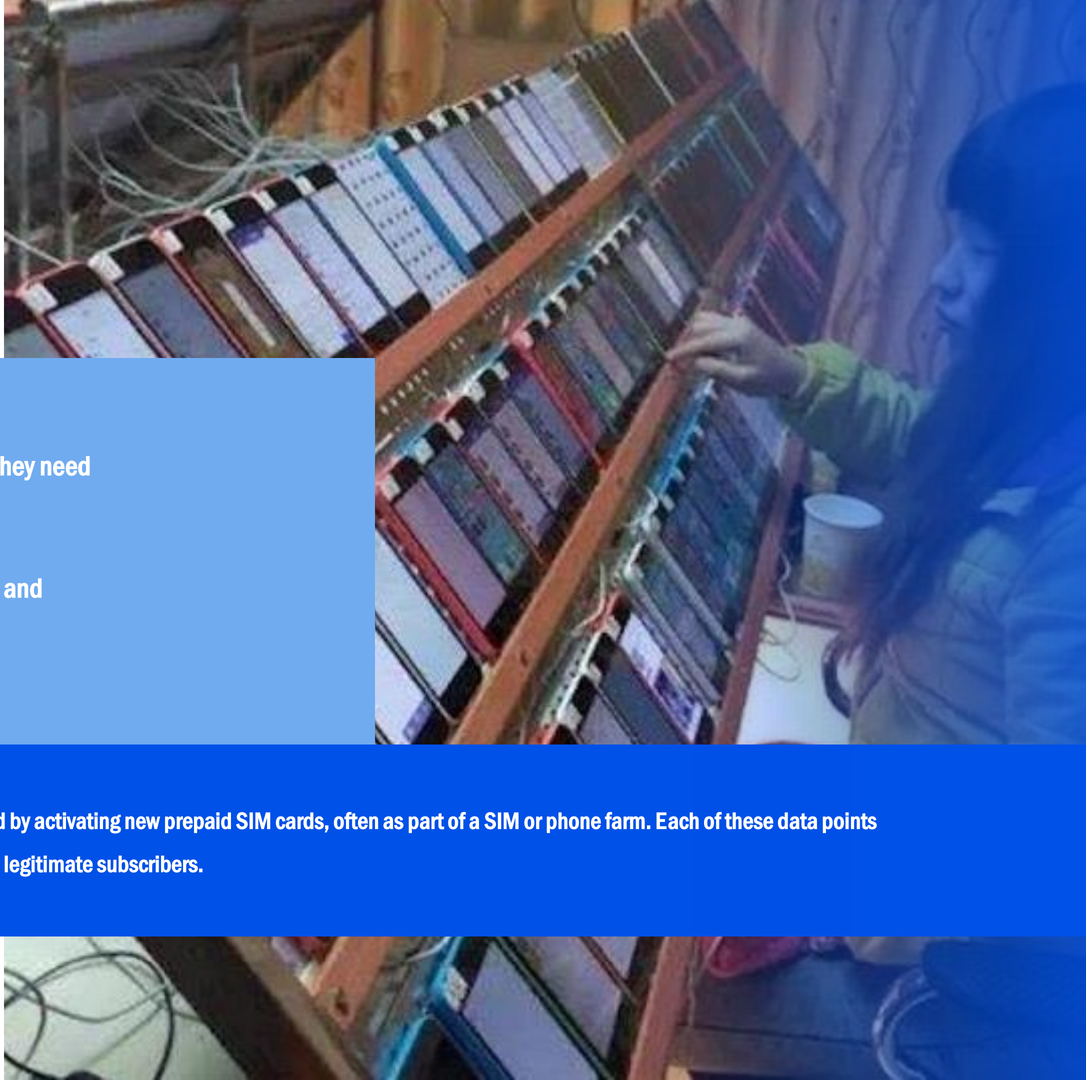
FRAUDSTERS CREATE FAKE ACCOUNTS TO:

- Spam
- Phish
- Fake listing
- Fake rides
- Post fake reviews
- Increase number of followers
- Use stolen credit cards
- Resell accounts
- Etc.

FARMING

To continue to create fake accounts, fraudsters have realized that they need access to thousands of mobile numbers.

Fraud is a business, so these mobile numbers must be anonymous and cheap/free for their business model to work.



Cheap/free mobile numbers are typically obtained by activating new prepaid SIM cards, often as part of a SIM or phone farm. Each of these data points helps to distinguish these “farmed” numbers from legitimate subscribers.

Data Point: Account Activation Date

DATA POINT

Date of Activation

- EXAMPLE: 2018-08-29

CLIENT TYPES

All that require phone number at registration

- Email
- Social media
- Ecommerce
- Gaming

DEMAND

High

VOLUME

Very high (billions/year)

- Would be used on every new registration

ELASTICITY

Medium/high

- If not available, alternative verification types will be used

Data Point: Contract Type

DATA POINT

Type of mobile phone contract

- EXAMPLE: Prepaid

CLIENT TYPES

All that require phone number at registration

- Email
- Social media
- Ecommerce
- Gaming

DEMAND

Medium/High

VOLUME

High

- Could be used on every new registration
- If used in conjunction with activation date, would likely be used only on newly-activated numbers

ELASTICITY

Medium/high

- While contract type is helpful, activation date may be sufficient for determining risk
- If not available, alternative verification types will be used

Thanks for joining. Your verification code is 675934

Fraud Alert – did you make a purchase of $399.82 today at 2:45 PM? Reply Y to confirm or N to deny

Arriving today: Your package... will be delivered by 8 PM. Track at t.ls/4Zly

Recycled Phone Numbers

FCC found that in the US 4.93% of users recycle their phone number each year

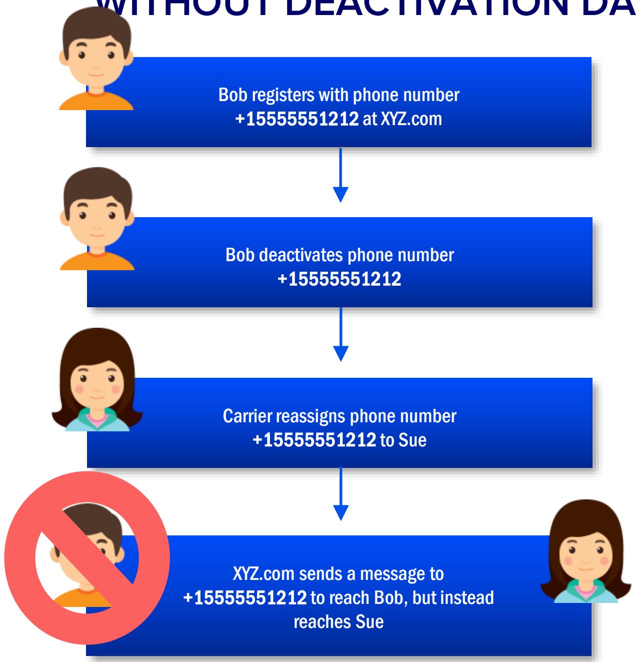
Phone verification during new account registration has become extremely popular. Websites and apps now rely heavily on their user's verified phone numbers for both **2FA** and **password reset** as previously described, and also for many communications use cases such as **account alerting**, **anonymous communications between users**, etc.

Because of this, it's extremely important that websites can trust that their users' phone numbers have not changed ownership. Otherwise, the website/app could be communicating with the wrong subscriber, causing frustration and annoyanceThis problem can be solved with a simple data point:

date of last deactivation

Date of Last Deactivation Usage Flow

WITHOUT DEACTIVATION DATE



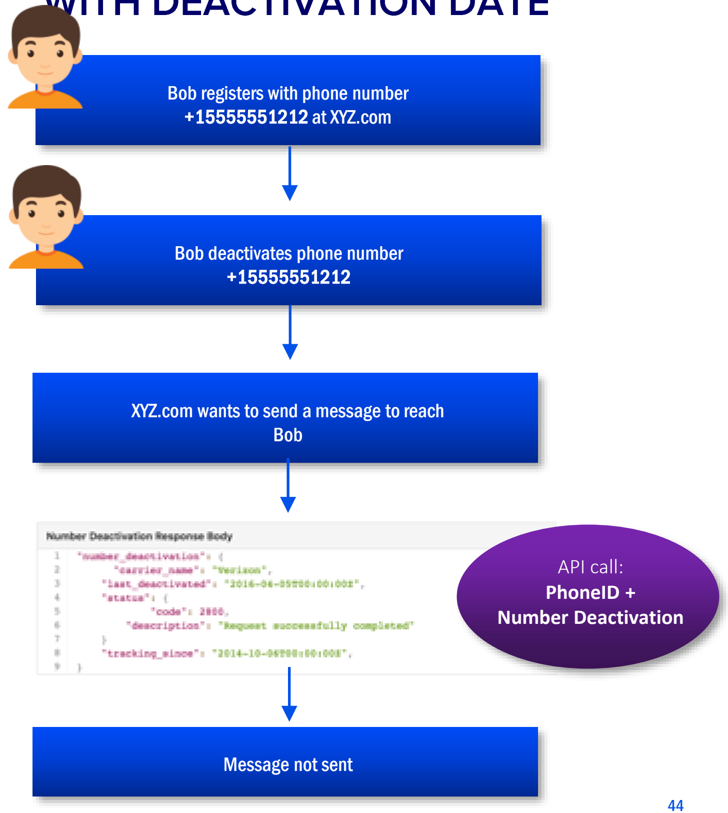
Bob registers with phone number +15555551212 at XYZ.com

Bob deactivates phone number +15555551212

Carrier reassigns phone number +15555551212 to Sue

XYZ.com sends a message to +15555551212 to reach Bob, but instead reaches Sue

WITH DEACTIVATION DATE



Bob registers with phone number +15555551212 at XYZ.com

Bob deactivates phone number +15555551212

XYZ.com wants to send a message to reach Bob

Number Deactivation Response Body

```
"number_deactivation": {
        "carrier_name": "Verizon",
    "last_deactivated": "2016-04-05T00:00:00Z",
    "status": {
            "code": 2800,
        "description": "Request successfully completed"
    }
    "tracking_since": "2014-10-06T00:00:00Z",
}
```

API call:
PhoneID + Number Deactivation

Message not sent

TeleSign

Data Point: Date of Last Deactivation/Recycling

DATA POINT

Date that the phone number was last deactivated

- EXAMPLE: 2018-08-29

VOLUME

Very High (billions of numbers)

CLIENT TYPES

All

ELASTICITY

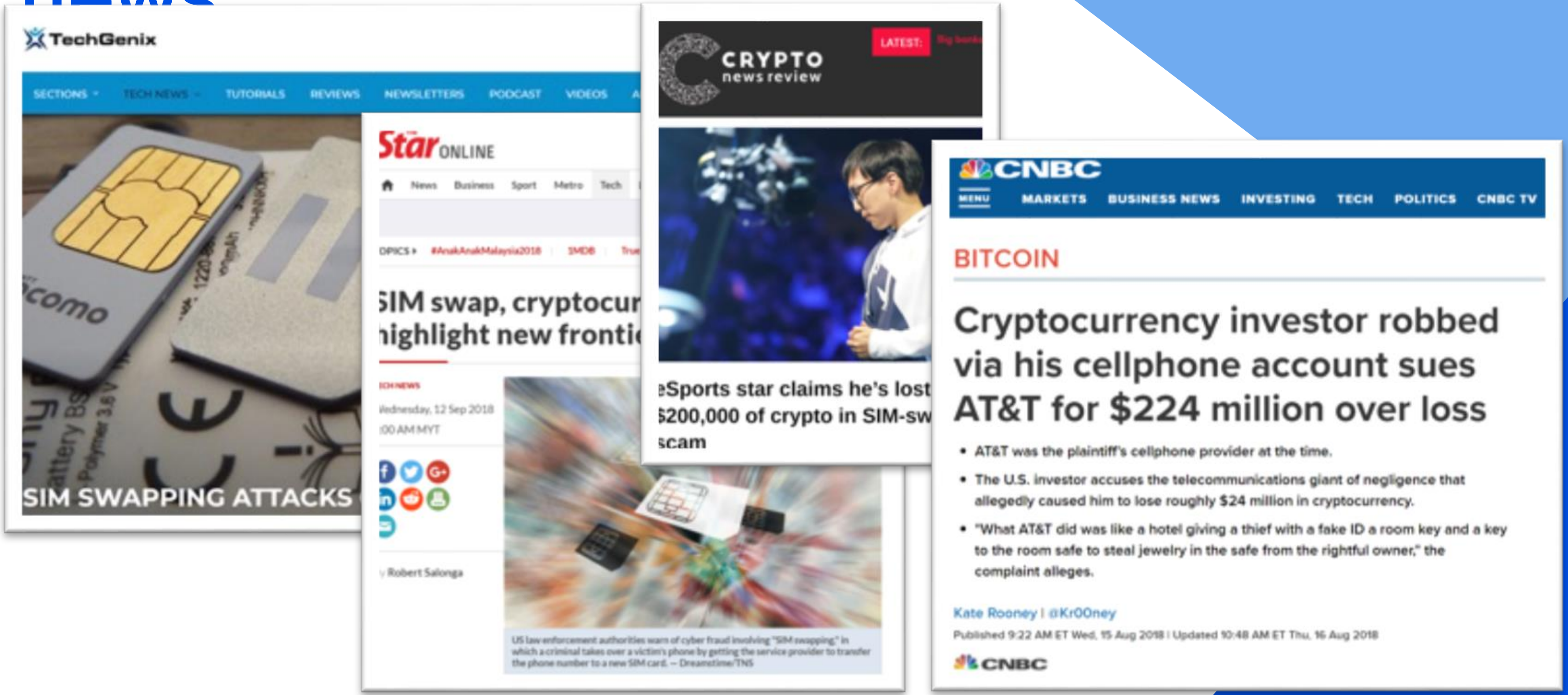
High

- If not available, websites will find other ways to mitigate the risks associated with a change of phone number ownership
- In addition, they may decide that phone numbers are not a reliable enough way to communicate with users

DEMAND

High

SIM Swap in the news



TechGenix

SECTIONS · TECH NEWS · TUTORIALS · REVIEWS · NEWSLETTERS · PODCAST · VIDEOS · A

SIM SWAPPING ATTACKS

Star ONLINE

News · Business · Sport · Metro · Tech

OPICS ▸ #AnakAnakMalaysia2018 | 1MDB | True

SIM swap, cryptocur
highlight new fronti

ECH NEWS

Wednesday, 12 Sep 2018
:00 AM MYT

y Robert Salonga

US law enforcement authorities warn of cyber fraud involving "SIM swapping," in which a criminal takes over a victim's phone by getting the service provider to transfer the phone number to a new SIM card. — Dreamstime/TNS

CRYPTO news review

LATEST:

eSports star claims he's lost
$200,000 of crypto in SIM-sw
scam

CNBC

MENU · MARKETS · BUSINESS NEWS · INVESTING · TECH · POLITICS · CNBC TV

BITCOIN

Cryptocurrency investor robbed via his cellphone account sues AT&T for $224 million over loss

- AT&T was the plaintiff's cellphone provider at the time.
- The U.S. investor accuses the telecommunications giant of negligence that allegedly caused him to lose roughly $24 million in cryptocurrency.
- "What AT&T did was like a hotel giving a thief with a fake ID a room key and a key to the room safe to steal jewelry in the safe from the rightful owner," the complaint alleges.

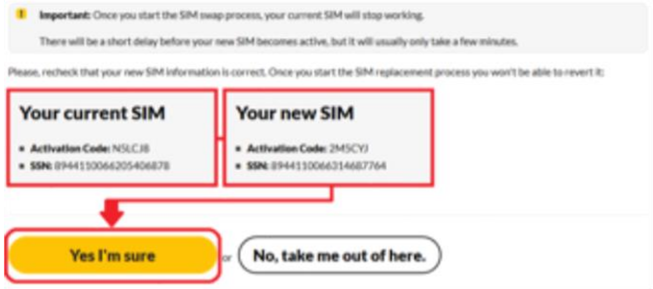
Kate Rooney | @Kr00ney

Published 9:22 AM ET Wed, 15 Aug 2018 | Updated 10:48 AM ET Thu, 16 Aug 2018

CNBC

SIM Swap: How it Works

- One way to hijack a user's phone number is via SIM swap
- The attack works like this:
  - The fraudster identifies the victim's phone number and phone carrier
  - He then poses as the legitimate user to the carrier, either in-store, on the phone, or online
  - The fraudster asks the carrier to transfer his (the victim's) phone number to a new SIM card because he lost his phone, etc.
  - The carrier transfers the phone number
  - The fraudster now has access to this phone number and receives the victim's 2FA codes when logging in online
- Knowing when the user activated his current SIM could stop this attack



Important: Once you start the SIM swap process, your current SIM will stop working.

There will be a short delay before your new SIM becomes active, but it will usually only take a few minutes.

Please, recheck that your new SIM information is correct. Once you start the SIM replacement process you won't be able to revert it:

Your current SIM

- **Activation Code:** NSLCJ8
- **SSN:** 8944110066205406878

Your new SIM

- **Activation Code:** 2M5CYJ
- **SSN:** 8944110066314687764

Data Point: SIM Swap Timestamp

DATA POINT

Timestamp of the activation of the current SIM card

- EXAMPLE: 2018-08-29 01:14:42

CLIENT TYPES

All that require phone number at registration

- Banks
- Cryptocurrency
- Ecommerce
- Email
- Social media

DEMAND

Financial/cryptocurrency companies: High

All others: Medium

VOLUME

Medium

- Likely only used on suspicious login attempts, where a user is trying to access his account from an unknown device and IP

ELASTICITY

Medium

- If not available, alternative verification types will be used

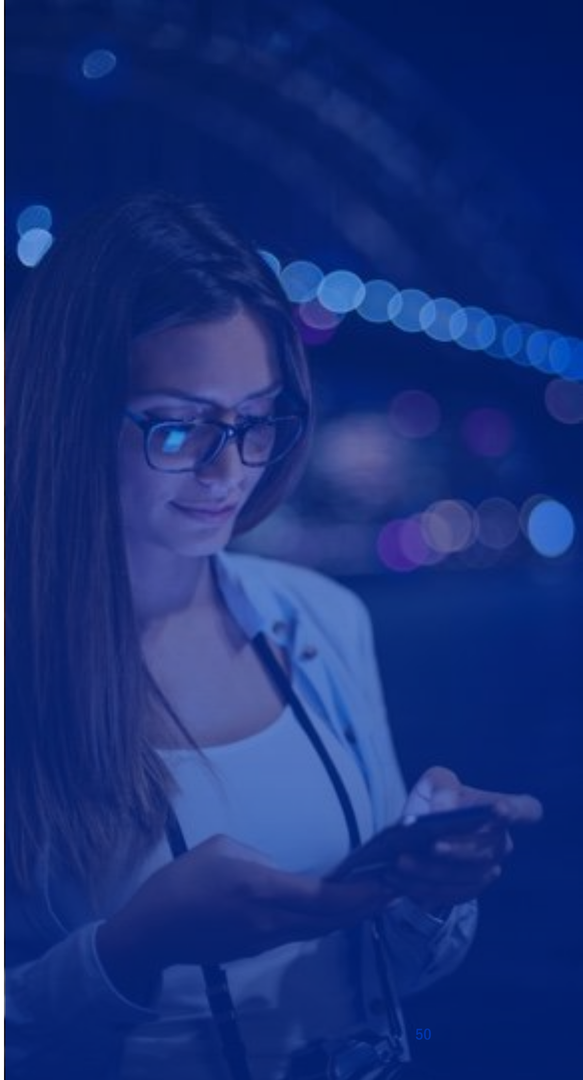
TeleSign

REASONS FOR ROLLOUT

Why Mobile Operators should embark on Mobile Identity ?

Protect your Users Online !!

- The role of carriers in keeping their subscribers' phone numbers secure is gaining attention – Competitive Differentiation
- There have been numerous high-profile stories recently about carriers giving fraudsters access to victim's phone numbers
- In August, it was reported that a cryptocurrency investor is suing AT&T for $224 million because AT&T allowed an unauthorized SIM swap
- As these stories gain publicity, subscribers lose confidence in their carriers' ability to keep their phone number safe
- There is **significant opportunity to be a carrier known for subscriber safety**, that subscribers can trust to keep them secure online



TeleSign

Recurring Revenue Opportunity

- Website and apps have spent the last several years adding phone numbers to all of their accounts
  - Now is the time to augment this phone number with additional information
- Every time a significant event happens with a phone number, there is an opportunity for data-related revenue
  - Registration for a new site
  - Login attempt
  - Password reset request
  - Identity verification needed
  - Phone number deactivated
- This opportunity should be acted on ASAP, before websites spend significant time and energy looking for new technologies to solve the challenges they're currently experiencing with phone number verification
- **Global Mobile Identity Opportunity – 30 Billion USD !!!**

TeleSign

A2P Traffic Growth

- Phone verification is currently driving much of the A2P traffic seen from websites and apps
  - Once a website has a user's verified phone number, they use it for 2FA, password reset, alerting, communications, etc.
  - Without a verified phone number, none of this A2P SMS traffic would exist
- If websites remain convinced that they can continue to rely on the phone number as a global identifier, they will continue to find reasons to communicate with their users via SMS

Embark on Mobile Identity Journey

Opportunity Assessments

Work with GSMA & Partners – TeleSign/BICS to understand opportunities

Assess Legal Readiness

Understand how other markets have managed Legal & Consent methods vis-à-vis your regulatory environment

Technical Readiness & POCs

Approach partners like TeleSign/BICS to perform POCs with live customers.

We are currently doing live POCs in EMEA, APAC & LATAM

Go Live

Sign commercial data partnerships with partners and local enterprises

Generate new Revenue !!

TeleSign

Start your Mobile Identity Journey today !!

rpatel@telesign.com

Thank you!

- Hangout recording available on: gsma.com/identity
- Identity at MWC19 Barcelona: Attend our seminars and visit us at the GSMA Innovation City
- Contact us at identity@gsma.com
- Follow us on LinkedIN (GSMA Identity)