#11 The positive impact of device intelligence

Wednesday 04 October
14:00 – 15:00 BST
<table>
<thead>
<tr>
<th>Time</th>
<th>Segment</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:00</td>
<td>Welcome and housekeeping</td>
<td>Conor Dempsey</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GSMA Services</td>
</tr>
<tr>
<td>14:05</td>
<td>The benefits of device intelligence for operators</td>
<td>Tyler Smith</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GSMA Services</td>
</tr>
<tr>
<td>14:15</td>
<td>How smartphone device intelligence helps improve business performance</td>
<td>Naser Al-Hasawi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zain Business</td>
</tr>
<tr>
<td>14:25</td>
<td>The new device status enhancements to combat device theft and fraud.</td>
<td>Jason Smith</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GSMA Services</td>
</tr>
<tr>
<td>14:35</td>
<td>The benefits of the reason codes to the GSMA Device Registry</td>
<td>Steve Schwed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verizon</td>
</tr>
<tr>
<td>14:45 – 15:00</td>
<td>Q&amp;A and closing remarks</td>
<td>Conor Dempsey</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GSMA Services</td>
</tr>
</tbody>
</table>
We play a vital role in the use of mobile device identifiers

TAC Allocations
The GSMA manage the industry’s global device identity scheme, called TAC. TAC is an 8-digit code which identifies all connected equipment types at product / brand level.

Device Identifiers
The GSMA holds highly accurate and unique data for over 8 billion devices for identification and verification purposes.

Device Status
Flag devices you own to indicate i) theft ii) fraud status to help block their use iii) trade iv) repair, v) subject to an ownership or financial claim.

Device Check
Check the status and history of an IMEI for real time ecommerce valuation purposes, and to identify fraudulent / irregular claims.

TAC = Type Allocation Code | OEM = Original Equipment Manufacturers | IMEI = International Mobile Equipment Identity

© GSMA 2023
Our Data Primary Source

- We hold the records of over 200K+ Type Allocation Codes
- Details of over 8 Billion devices

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Available device attributes / properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile / Feature Phone</td>
<td>Manufacturer, consumer recognized marketing name, model name, brand name, year released</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Device type (M2M device, Tablet, Smartphone, Watch, etc.), screen size, chipset, CPU, clock speed, RAM, VoLTE enabled, IoT endpoint, IoT enabler, IoT controller</td>
</tr>
<tr>
<td>Tablet</td>
<td>Operating System name and minimum OS version (e.g. Android 8, iOS 11, etc.)</td>
</tr>
<tr>
<td>IoT Device</td>
<td>Network Protocols: 2G, 3G, 4G, 5G, LTE Category, VoLTE, VoWiFi</td>
</tr>
<tr>
<td>Wearable</td>
<td>Browser: Name, version, rendering engine, etc.</td>
</tr>
<tr>
<td>Dongle</td>
<td>HTML5: CSS, HTML5 properties</td>
</tr>
<tr>
<td>Modem</td>
<td>Multimedia: Streaming, Audio, Video codecs, Bluetooth</td>
</tr>
<tr>
<td>WLAN Router</td>
<td></td>
</tr>
</tbody>
</table>
Our device intelligence is used in several industry sectors

- Device Traders
- Government and Regulators
- Insurers
- MNO/MVNO
- Mobile Application/Software
- Retailers

Benefits to customers

- Accurate and fast device identification on networks assists in network rollout / sunsetting of proper subscription rates
- Quickly verify device legitimacy at ports of entry
- Integration of our device data with internal analysis and workflows brings incremental value, i.e., determining an upsell campaign or valuation of a device
GSMA TAC based data service types

**GSMA Device Database**

- 10,000+ device models launched every year
- 10,000+ device models in the database
- 1 global source of device manufacturers

**GSMA Device Map**

- 150+ curated device capabilities
- 20+ IoT device-type classifications
- Mapped over GSMA TAC Data

- 2G-5G manufacturer and model identification
- Uplink/downlink MIMO and QAM band performance
- Operating system identification
- 2G-5G manufacturer, model, and marketing identification
- Consumer IoT vs M2M device monitoring
- Chipset and browser HTTP protocol
- Uplink/downlink MIMO and QAM band performance
Service delivery and data ingestion

- Secure end point connection
  - Daily updates
  - Automation of file retrieval
  - Delta reporting
- General Web Portal Access
- Scoping real-time API for tighter and more seamless integrations
Introduction – About Myself

NASER SALEM ALHASAWI
Business Insights & Analytics Department Manager
Business Intelligence Division
Zain Kuwait

2003
BS Computer Engineering
California State University, Chico

2004 – 2005
Instrument Engineer
Ministry of Electricity and Water (MEW)

2006 - 2016
Network - Value Added Service Engineer
Zain Kuwait

2017 - Present
Business Insights and Analytical Manager
Zain Kuwait
Introduction – About Zain

Mobile Telecommunications Company - Zain was founded in 1983 in Kuwait as the first telecom operator in the Middle East and Africa.

The Group’s flagship operation has enjoyed a proud history of achievements since then, including becoming the first operator to launch a commercial GSM service in the region in 1994, as well as becoming the first company in Kuwait to launch nationwide 4G LTE Internet services in 2012. In 2019, Zain announced its network was fully ready for the commercial launch of fifth generation wireless technology (5G) to be the first operator to offer 5G in the GCC region via the Kuwaiti market with nationwide coverage of all areas.
**Background – Prior To Current State**

1. **Generate Device Mapping** – Once A Month
2. **Upload To FTP Folder**
3. **Sanity Checks & Fixes**
4. **Run Loading Process**
5. **Ready For Use**

Start → Upload To FTP Folder → Sanity Checks & Fixes → Run Loading Process → Ready For Use
Nearby Past – Motivation To Move Current State

- Accurate and Trusted
- Enable automation and integration
- Shorten analysis & insights cycle
- Information is up to date
- Rich in features
Today – Sample of achieved applications, with approved & up-to-date device information, many reliable insights and data initiative being generated.

**Insights & Analytics**
- Key input in many reports, dashboards, and machine learning models
- Device level segmentation and customer device history

**Network Focused Use-Cases**
- 2/3G network decommission initiative
- Device level network experience

**Marketing, IoT, Product & Services**
- Track demand & forecast
- Monitored new device launched
- Identify preferred market preference from different device information prospective i.e IoT
- Device triggered campaign

**Government & Regulatory**
- Device information for security requests
- Device & Smartphones market penetration
Trusted, active, and enriched devices' information capability is now a basic need for us to help understand customers and meet expectations.

Thank You
We play a vital role in the use of mobile device identifiers

**TAC Allocations**

The GSMA manage the industry’s global device identity scheme, called TAC. TAC is an 8-digit code which identifies all connected equipment types at product / brand level.

86 916102

**Device Identifiers**

The GSMA holds highly accurate and unique data for over 8 billion devices for identification and verification purposes.

**Device Status**

Flag devices you own to indicate i) theft ii) fraud status to help block their use iii) trade iv) repair, v) subject to an ownership or financial claim.

**Device Check**

Check the status and history of an IMEI for real time ecommerce valuation purposes, and to identify fraudulent / irregular claims.

TAC = Type Allocation Code | OEM = Original Equipment Manufacturers | IMEI = International Mobile Equipment Identity

© GSMA 2023
GSMA device validation service types

GSMA Device Registry

Be part of the collective fight against device crime. Flag fraudulent and stolen devices through the world’s most accurate device registry.

+100 million devices have been flagged
+1 million fraudulent/stolen devices blocked
+150 companies in our community

GSMA Device Check™

Protect against the risk of handling stolen or fraudulent devices. By instantly checking a device’s status, through the world’s most accurate device registry.

+100 million look-ups per year
7 YEARS of a device’s history
10 insights on device model and capabilities
Device status intelligence

Contributors

Insurer
Retailer
Distributor
OEM
MVNO

Network Operators Access
Device Status Exchange
• 120+ Mobile Network Operators
• 42 countries
• help protect 1+ billion users

Safer Device Trading Capability
GSMA Device Check™
• Entire Device Ecosystem
• 250+ organisations
• 50+ countries
• 100+ million devices queried per year
GSMA Device Registry use cases

Lost or Stolen
Not with rightful owner

Fraudulently Obtained
Obtained with no intent to pay

Broken or Faulty
Technical and/or safety issue

Court Ordered Block
• MNO use only
• Legal obligation

Ownership Claim
• Assert ownership
• Prevent unapproved trade

Financial Claim
• Assert financial claim
• Prevent premature trade

Block trade and use (Block List)

Consider further investigation (General List)
Ownership + Financial claim use case examples

Ownership Claim

1. Purchase inventory
2. Flag devices
3. Lease device to customer
4. Customer files insurance claim
5. Insurer’s GSMA Device Check™ query results prevent fraud / loss

Financial Claim

1. Device sold with financing
2. Flag device
3. Customer seeks to sell device before paying balance
4. Buyer’s GSMA Device Check™ query results cause seller to pay balance before trade
5. Buyer and seller complete trade
GSMA Device Check™ API response example

```json
{
  "refcode":"29022016012620",
  "responsestatus":"success",
  "deviceid":"35765206726822",
  "partnerid":"Acme Ltd",
  "blockliststatus":"No",
  "generalliststatus":"Yes",
  "imeihistory":{
    "action":"General Insert",
    "reasoncode":"0042",
    "reasoncodedesc":"Ownership Claim",
    "date":"2022-06-15 16:37:12.0",
    "by":"Mobile Device Sales, Inc.",
    "Country":"United States"
  },
  "manufacturer":"Sony Mobile Communications",
  "brandname":"Sony",
  "marketingname":"Xperia Z3 Compact",
  "modelname":"M55w, D5803",
  "band":"LTE FDD BAND 7, LTE FDD BAND 13, WCDMA FDD Band 1, WCDMA FDD Band VIII, LTE FDD BAND 20, LTE FDD BAND 5, LTE FDD BAND 2, GSM 900, LTE FDD BAND 3, LTE FDD BAND 4, LTE FDD BAND 17, GSM 1800, LTE FDD BAND 1, LTE FDD BAND 8, WCDMA FDD Band II, WCDMA FDD Band IV, WCDMA FDD Band V, GSM850 (GSM800)",
  "operatingsys":"Android",
  "nfc":"Yes",
  "bluetooth":"Yes",
  "WLAN":"Yes",
  "devicetype":"Smartphone"
}
```
About the Speaker...

Steve Schwed

Vice President | CFCA

Verizon | Fraud Strategy Manager


In addition, Steve was responsible for maintaining the relationship and service level commitments for responses to consumer complaints for the various Attorneys General, The FCC and other regulatory and consumer advocacy groups.

Steve’s involvement with Telecommunications Fraud began in 2013 while working as a Process Manager in the VZW Customer Service Group and was tasked with addressing issues related to Loss and Policy. Steve officially joined Verizon's Fraud Strategy Team in 2015. He is a member of various GSMA Forums and member of the CFCA and co-chairs the CFCA Handset Trafficking Taskforce.

Steve holds a bachelor’s degree in Economics and speaks frequently regarding handset Fraud Losses.
Abbreviated Discussion Points

Block List penetration in the industry and use of the Reason Codes
Brief Discussion on US Carrier Participation in 2022 and the need to expand the number of participants to include OEMs as well as more carriers to make the process more effective

IMEI hardening
Continue previous industry discussions on what could be done to prevent not only IMEI obfuscation but improve the ability of OEMs to potentially reduce counterfeit device production

US Stolen Phone Legislation CTIA Stolen Phone Working Group.
Update on the current ongoing work with the CTIA SPWG to create meaningful Laws in the US to prevent offering services such as removing devices from the Negative lists, IMEI overwriters and SIM cover import and distribution along with advertising for these services.
US Carriers are not using the GSMA Block List reason codes consistently, allowing certain restricted devices “On Network”

Since inception of the Fraud Reason Code in 2018, not all carriers were using “Fraudulently Obtained” or the more recent “Court Ordered” reason codes, nor did they appear to be blocking the listings .... Until recently

Results from 2022 the GSMA Annual Report on Blocklisting showed the following data:

<table>
<thead>
<tr>
<th>Carrier</th>
<th>Stolen / Lost 11,14</th>
<th>Fraudulently Obtained 26,27</th>
<th>Court Ordered 28,29</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>T Mobile</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sprint (TMO)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Verizon</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Increased use of the Lost and Stolen reason codes was believed to be due to lack of carrier participation than in fraud codes outside of US – greater alignment is needed to properly report consumer theft numbers.

Greater alignment by carriers GLOBALLY is needed to improve consistency.
The visual and the questions ....

- Are carriers properly identifying the hallmarks of Synthetic ID Fraud?
- Are carriers not acknowledging Fraud Losses (reporting or subscribing to fraud being reported by other carriers)?
- What can be done to attain greater alignment in the US and Foreign markets?
- If greater participation doesn’t occur, will carriers participate with greater scrutiny of their partners?
- Will OEMs start to look at the Fraud Reason code for Bricking devices (Non consumer)
Are OEMs and the industry working to solve for IMEI hardening or are they stymied for a solution?

Recent arrests in Money Laundering Cases (Not device trafficking or stolen device possession) in the US has provided insights that IMEI manipulation and replacement is occurring, and organized criminals are attempting to prevent detection of stolen and fraudulently obtained devices.

Investigators shared that IMEI over writers were found and used in the Houston Operation of “We Buy Phones”.

Hardening or protecting an IMEI would not only prevent IMEI obfuscation but could also prevent the counterfeiting of devices.

Making it harder to hide the identity of a device will make it easier to prosecute criminals.
How might we harden an IMEI?

What an IMEI solution incorporating attestation via a Security Token (or One Time Password) specific for the IMEI might look like:

Could an alternate to designing a “write once” method for IMEI’s be solved for with Authentication?

Without duplicating the Token Generator to match the OEM server exactly, counterfeiting could be substantially reduced.

OEM Disablement of the Device for Manipulation or Fraud Concern

Verification Confirmed

Verification Failure

All verification done behind the scenes — no customer Interaction Required

IMEI

IMEI 35123456789101112

Token or OTP Generator (on handset)

IMEI And OTP must be paired (Attestation)

Could an alternate to designing a “write once” method for IMEI’s be solved for with Authentication?
US Stolen Phone Legislation

Work began in 2020 by the CTIA Stolen Phone Working Group to try and update the latest version of the US Code to implement the “Stop Stolen Mobile Device Trafficking Act”

• Numerous Sessions with Senator Chuck Schumer’s office have been supportive, but have yet to yield a formal introduction to the US Senate- (there is still work to do)

• Act looks to restrict the advertising, distribution and sale of equipment or services designed to:
  - Alter an IMEI or any other method of changing the network performance of the Handset (Such as a SIM lock or Blocklist listing
  - Sale, Import or distribution of devices to alter an IMEI or how a SIM operates
  - Creates a punishable offense for advertising for sale or purchase “Blocklisted” devices and for the trafficking of device lost to theft or fraud

Challenges:

• Multiple delays due to COVID and COVID related legislative efforts
• Varying definitions of Fraud from Country to Country
• Stalemate with Right to Repair Lobbyists
In summary...

There is no single solution to solve for fraud

- We need to look at enhanced implementation of the blocklists
- Respond faster to fraud strategy of the bad actors
- Continue to pressure regulators and legislators as to the true challenges and question the Status Quo
  - Update the Laws (US -written over 10 years ago)
  - Partner with the proper legislators to advance legislation
  - Expand the legislation to other countries
- Update technology to make sharing block data more cost effective and inviting to smaller carriers
Thank you for joining, any questions?