

GSMA
Services Showcase
LIVE

#11 The positive impact of device intelligence

Wednesday 04 October
14:00 – 15:00 BST

© GSMA 2023



GSMA™

Agenda

Time	Segment	Speaker
14:00	Welcome and housekeeping	Conor Dempsey GSMA Services
14:05	The benefits of device intelligence for operators	Tyler Smith GSMA Services
14:15	How smartphone device intelligence helps improve business performance	Naser Al-Hasawi Zain Business
14:25	The new device status enhancements to combat device theft and fraud.	Jason Smith GSMA Services
14:35	The benefits of the reason codes to the GSMA Device Registry	Steve Schwed Verizon
14:45 – 15.00	Q&A and closing remarks	Conor Dempsey GSMA Services

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

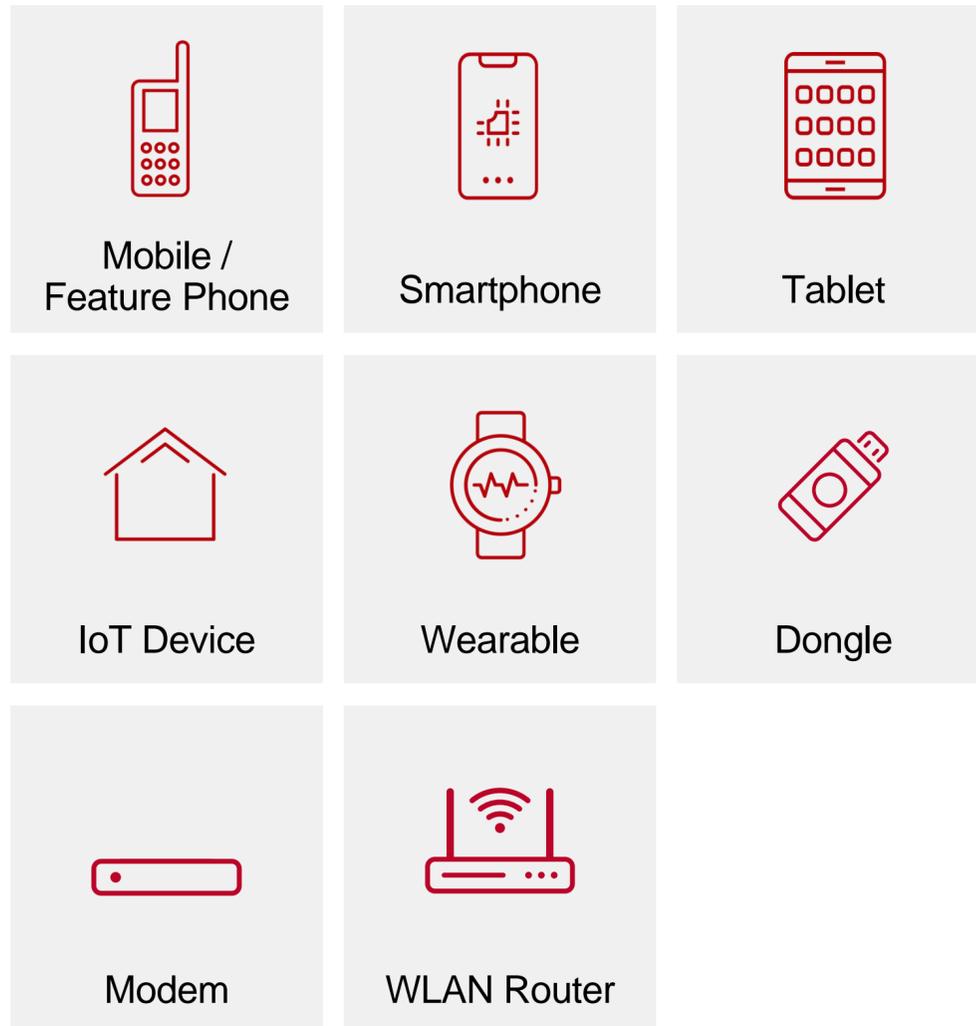
Check the status and history of an IMEI for real time ecommerce valuation purposes, and to identify fraudulent / irregular claims



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

Our Data Primary Source

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



Type Allocation Code (TAC)

86	916102	991292	0
Reporting Body Identifier	Type Identifier indicating brand owner and device model allocated by Reporting Body	Unique Number assigned to individual devices by the manufacturer	Check Digit A function of the other digits [calculated by the manufacturer]

International Mobile Equipment Identifier (IMEI)

The 8-digit **TAC** identifies the brand owner, model and marketing name

The 15-digit **IMEI** identifies the individual device when seen on a network

Device Category	Available device attributes / properties
Device Identification	Manufacturer, consumer recognized marketing name, model name, brand name, year released
Hardware Information	Device type (M2M device, Tablet, Smartphone, Watch, etc.), screen size, chipset, CPU, clock speed, RAM, VoLTE enabled, IoT endpoint, IoT enabler, IoT controller
Operating System	OS name and minimum OS version (e.g. Android 8, iOS 11, etc.)
Network Protocols	2G, 3G, 4G, 5G, LTE Category, VoLTE, VoWiFi
Browser	Name, version, rendering engine, etc.
HTML5	CSS, HTML5 properties
Multimedia	Streaming, Audio, Video codecs, Bluetooth

GSMA's device data overview

Our device intelligence is used in several industry sectors

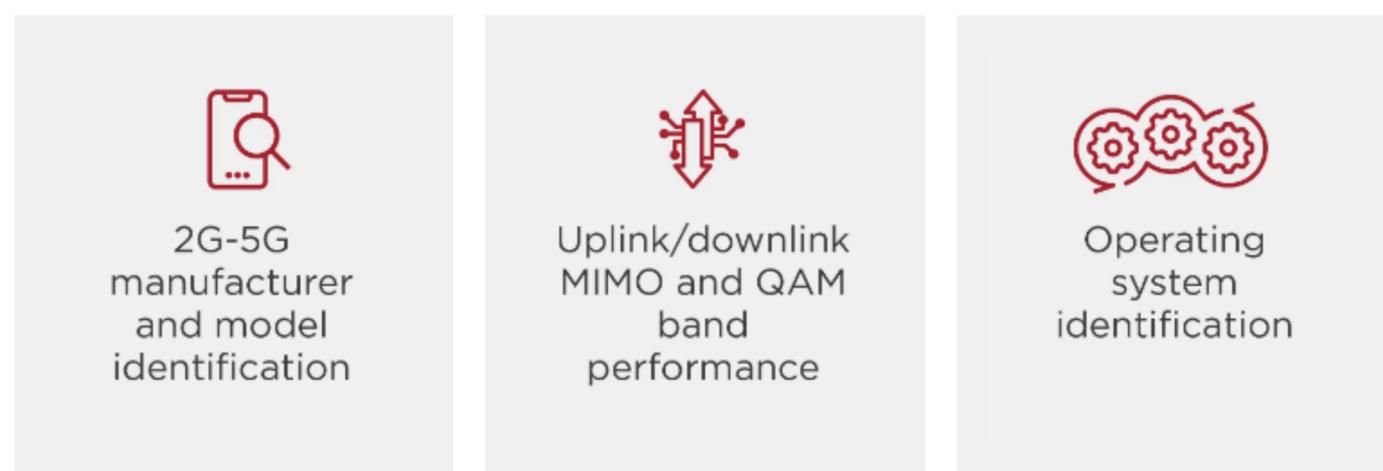
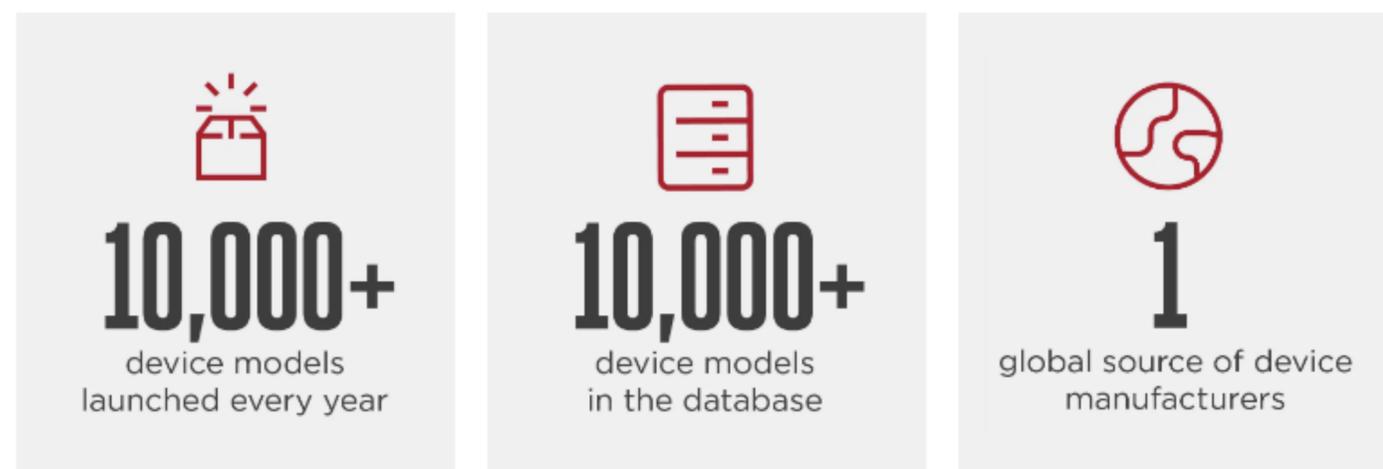
-  Device Traders
-  Government and Regulators
-  Insurers
-  MNO/MVNO
-  Mobile Application/Software
-  Retailers

Benefits to customers

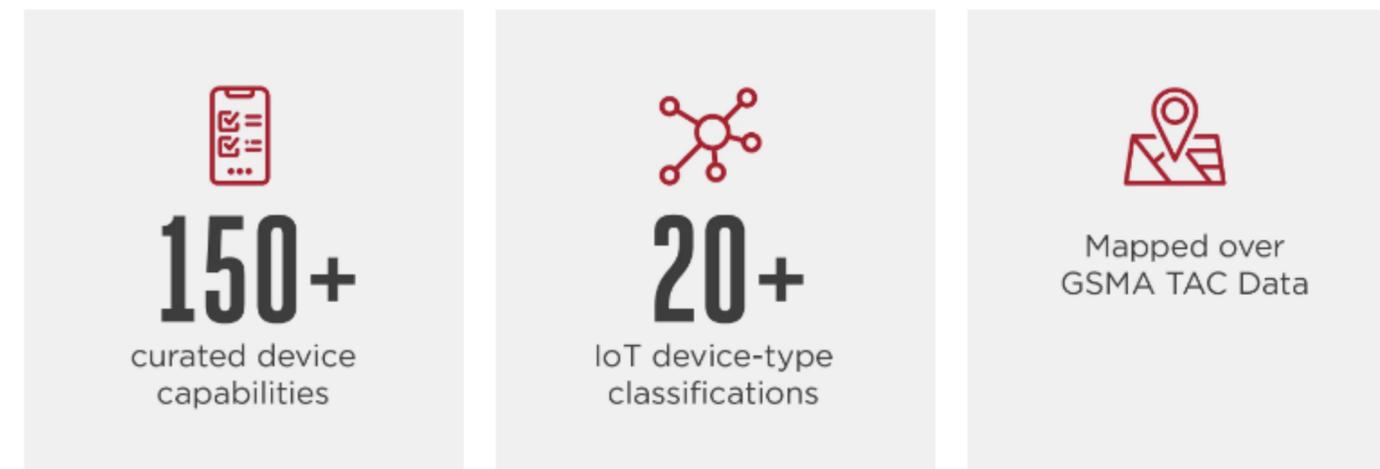
- Accurate and fast device identification on networks assists in network rollout / sunsetting of proper subscription rates
- Quickly verify device legitimacy at ports of entry
- Integration of our device data with internal analysis and workflows brings incremental value, i.e., determining an upsell campaign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

GSMA TAC based data service types

GSMA Device Database



GSMA Device Map





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

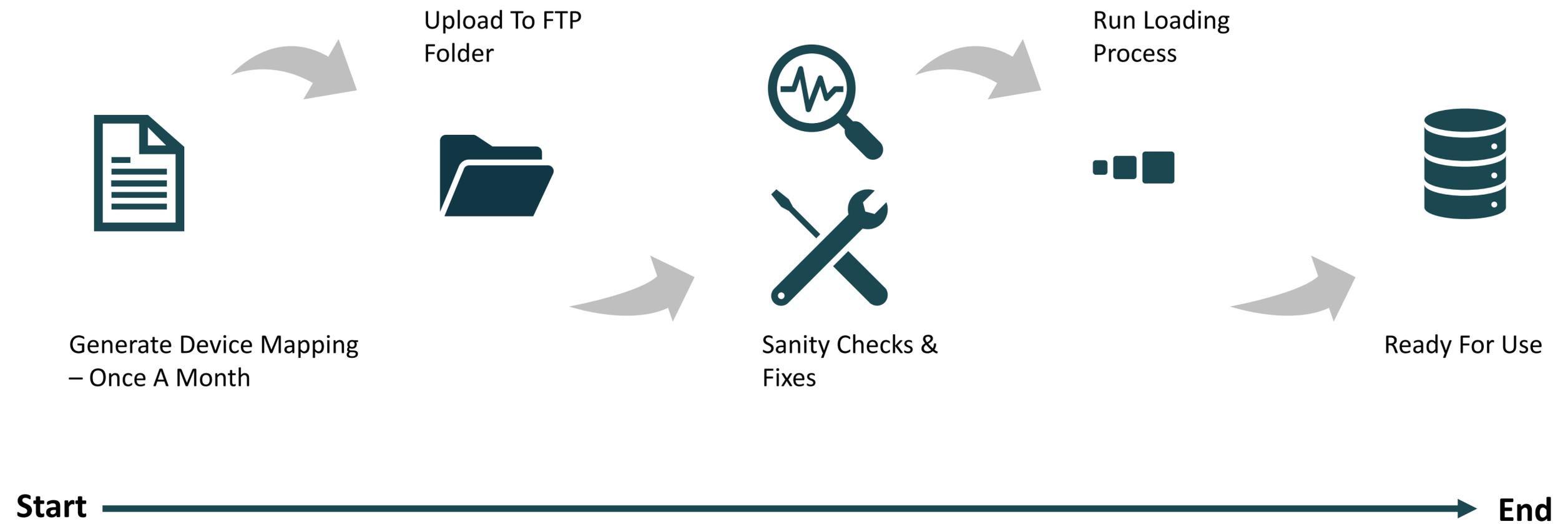
Introduction – About Zain



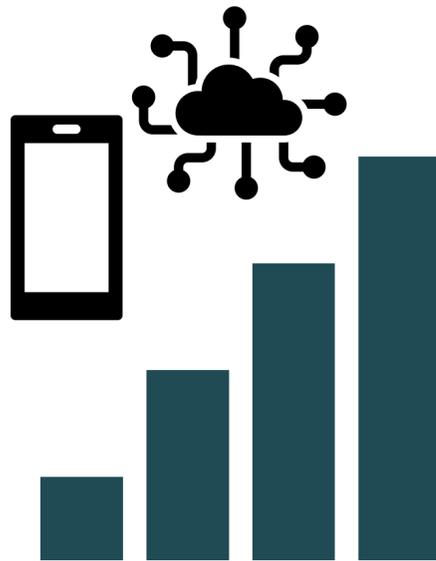
Mobile Telecommunications Company - Zain was founded in 1983 in Kuwait as the first telecom operator in the Middle East and Africa.

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



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

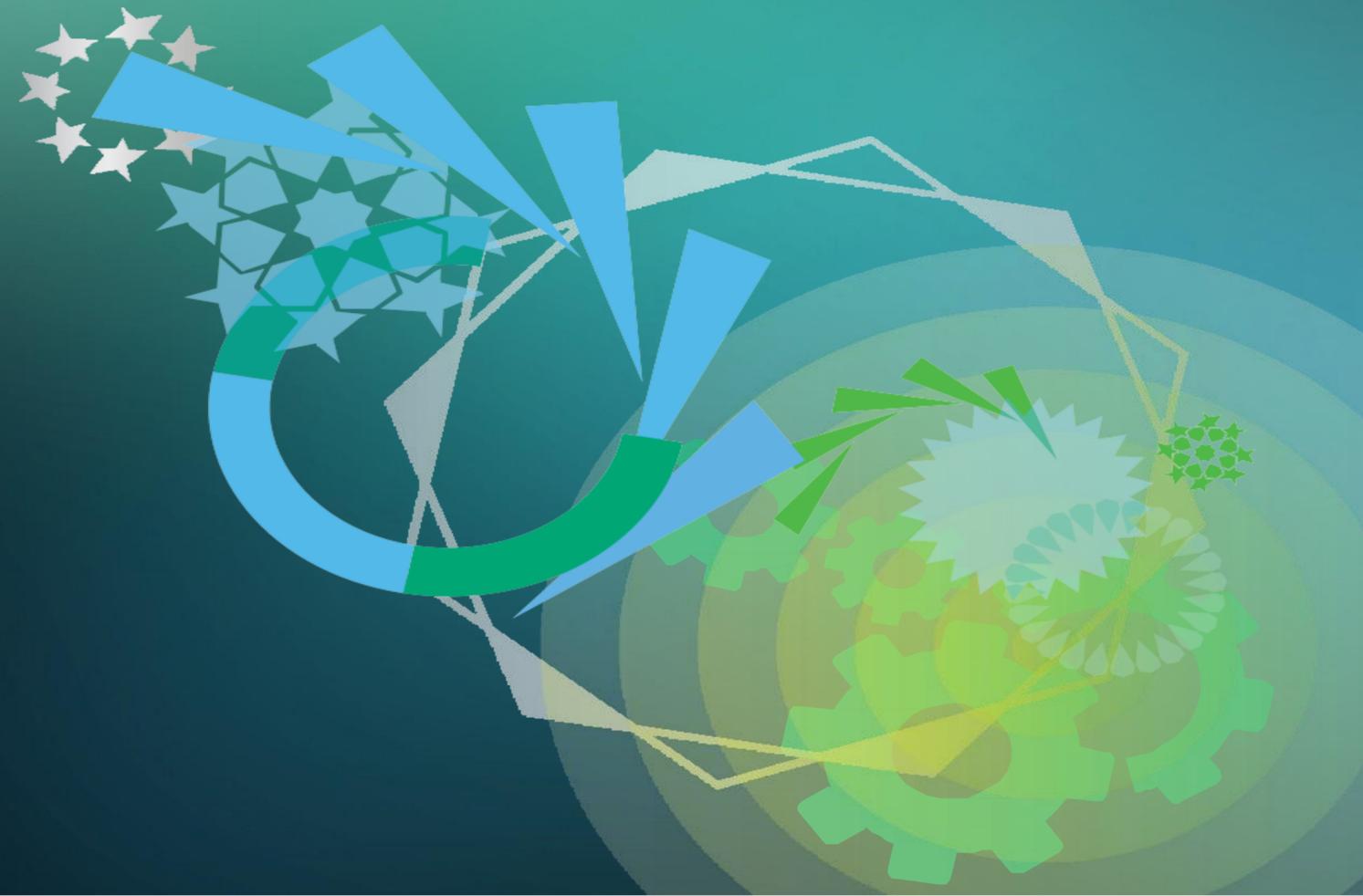
- Track demand & forecast
- Monitored new device launched
- Identify preferred market preference from different device information prospective i,e IoT
- Device triggered campaign

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



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 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

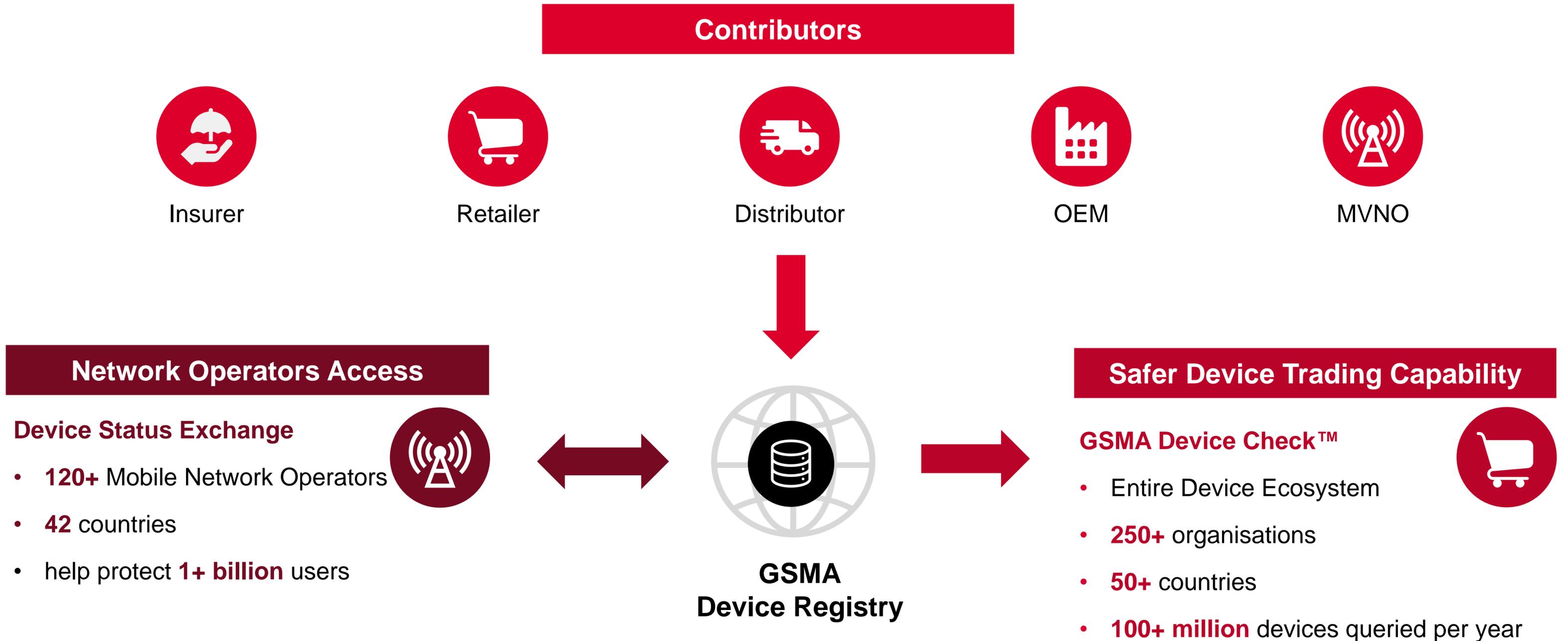
of a device's history



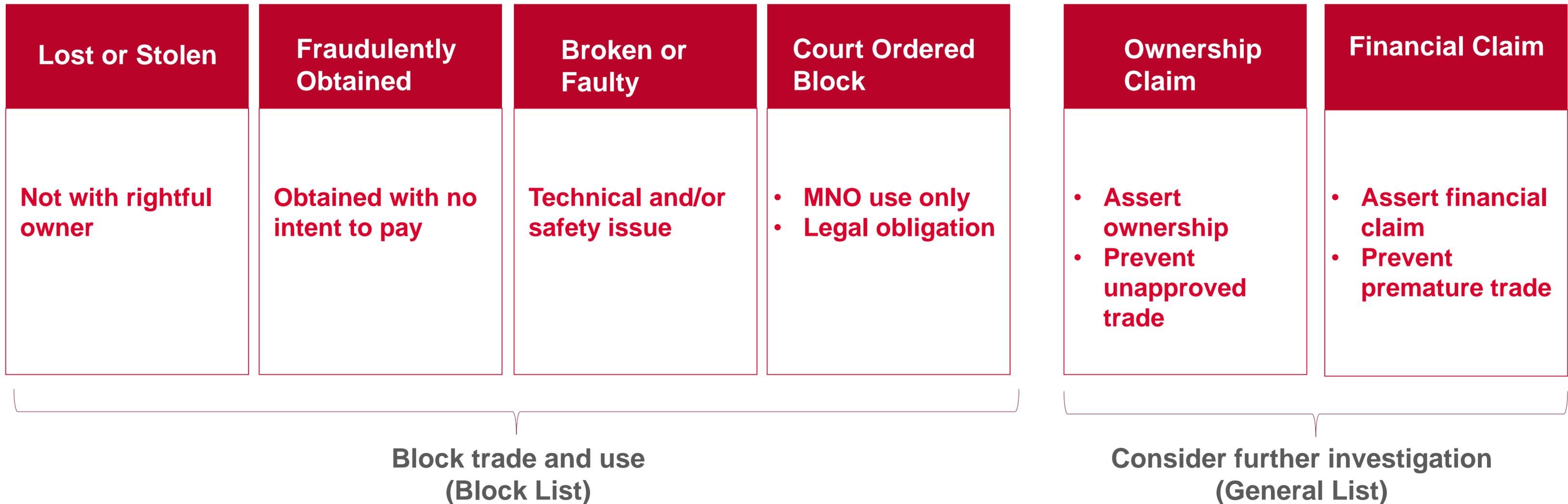
10

insights on device model and capabilities

Device status intelligence

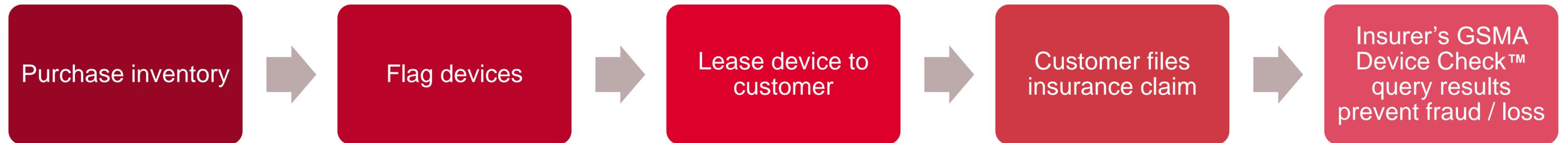


GSMA Device Registry use cases

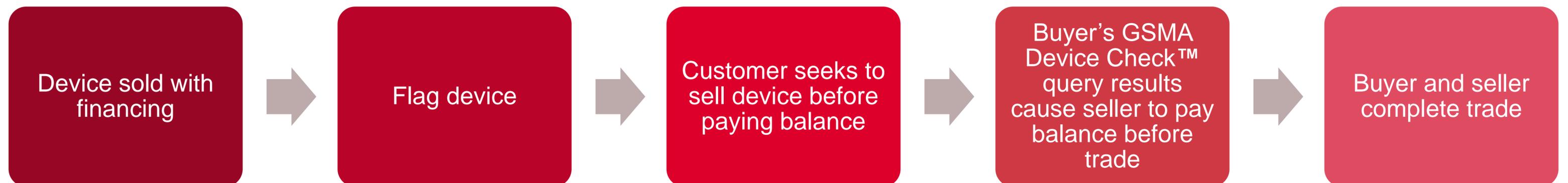


Ownership + Financial claim use case examples

Ownership Claim



Financial Claim



GSMA Device Check™ API response example

Your Results

Organisation Details

Organisation Name	GSM Ops	Organisation Id	310/RTPC/[REDACTED]
Organisation Country	United States	Date Of Check	09-23-2023 11:06:13
Checked By	[REDACTED]		

Number Checked

IMEI	357652 [REDACTED]
Device Status	⚠ On Block List ✔ Not on General List

```
{
  "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 I, 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 | CFCFA

Verizon | Fraud Strategy Manager



Steve began his career in telecommunications in 1997 with Bell Atlantic Mobile in their Customer Financial Services group before assuming responsibility for the Executive Relations group for the Philadelphia Region in 2000 followed by managing the Verizon Wireless National Executive Relations Team from 2005 until 2013.

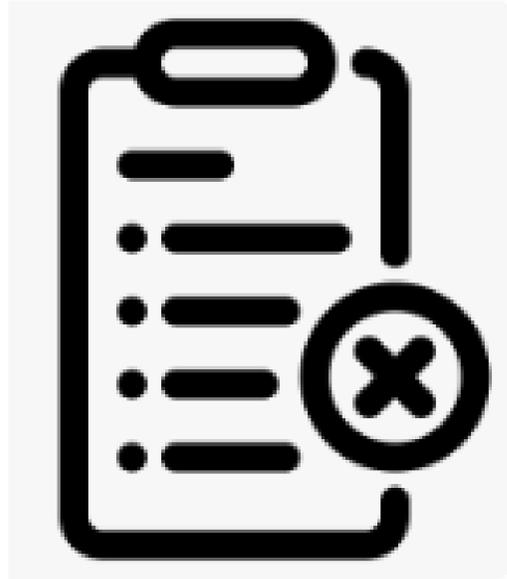
In addition, Steve was responsible for maintaining the relationship and service level commitments for responses to consumer complaints for the various Attorneys General, The FCC and other regulatory and consumer advocacy groups.

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 CFCFA and co-chairs the CFCFA 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

IN THE SENATE OF THE UNITED STATES

XXXXXXXX, 2022

A BILL

of and commerce in stolen mobile devices by making it unlawful to alter o
quipment identification number of a mobile device, and by making it unlaw
: devices that have been ~~lost~~, ~~stolen~~, or fraudulently obtained.

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:

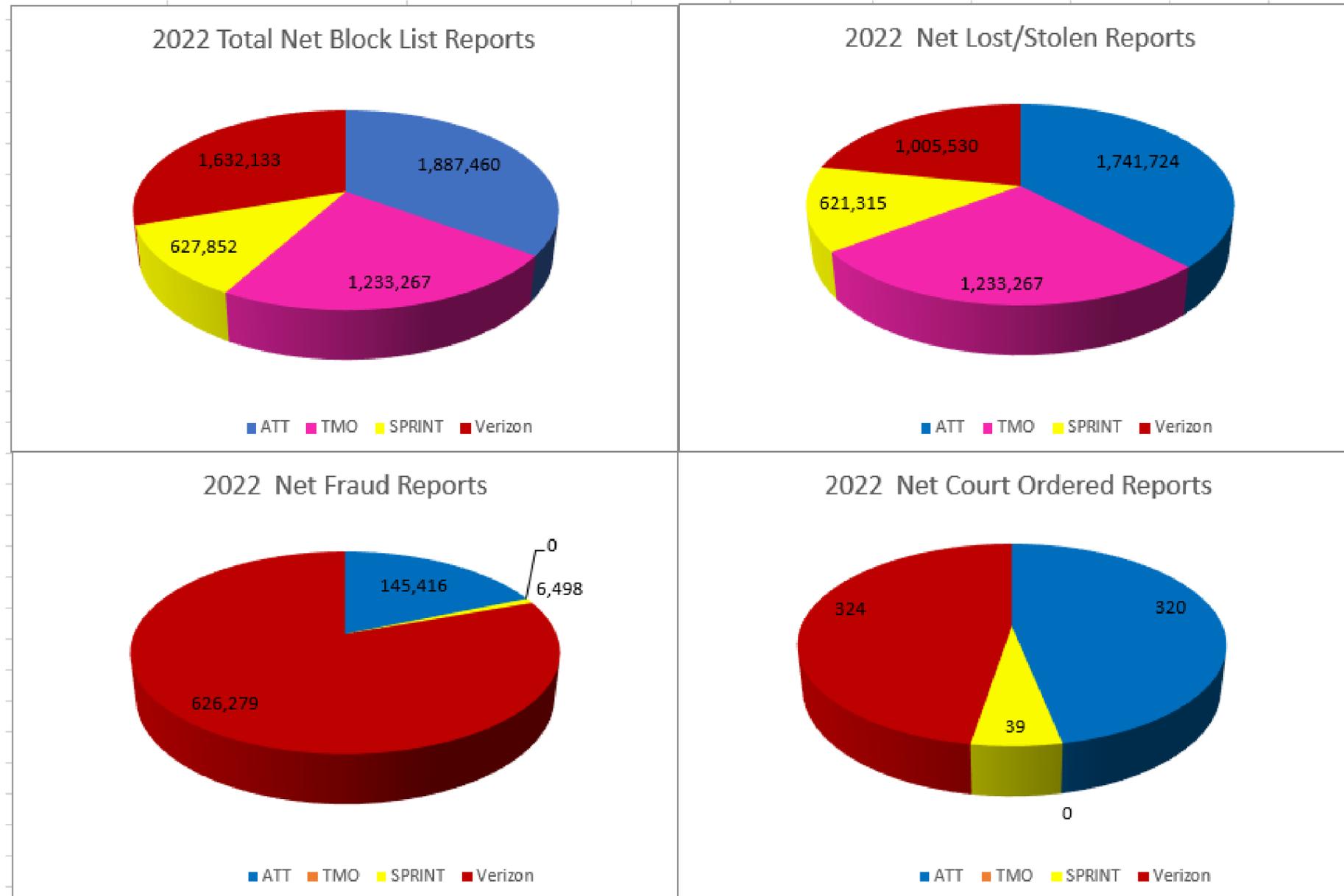
	Stolen / Lost 11,14	Fraudulently Obtained 26,27	Court Ordered 28,29
AT&T	Yes	Yes	Yes
T Mobile	Yes	No	No
Sprint (TMO)	Yes	Yes	Yes
Verizon	Yes	Yes	Yes

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.



MONEY LAUNDERING

\$1.8M worth of stolen devices found in organized crime ring bust in Houston area, investigators say

HOUSTON, Texas (KTRK) -- Three people are under arrest in connection to a \$65 million organized crime and money laundering scheme that has fueled many recent cellphone robberies and thefts in the Houston area, investigators said.

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

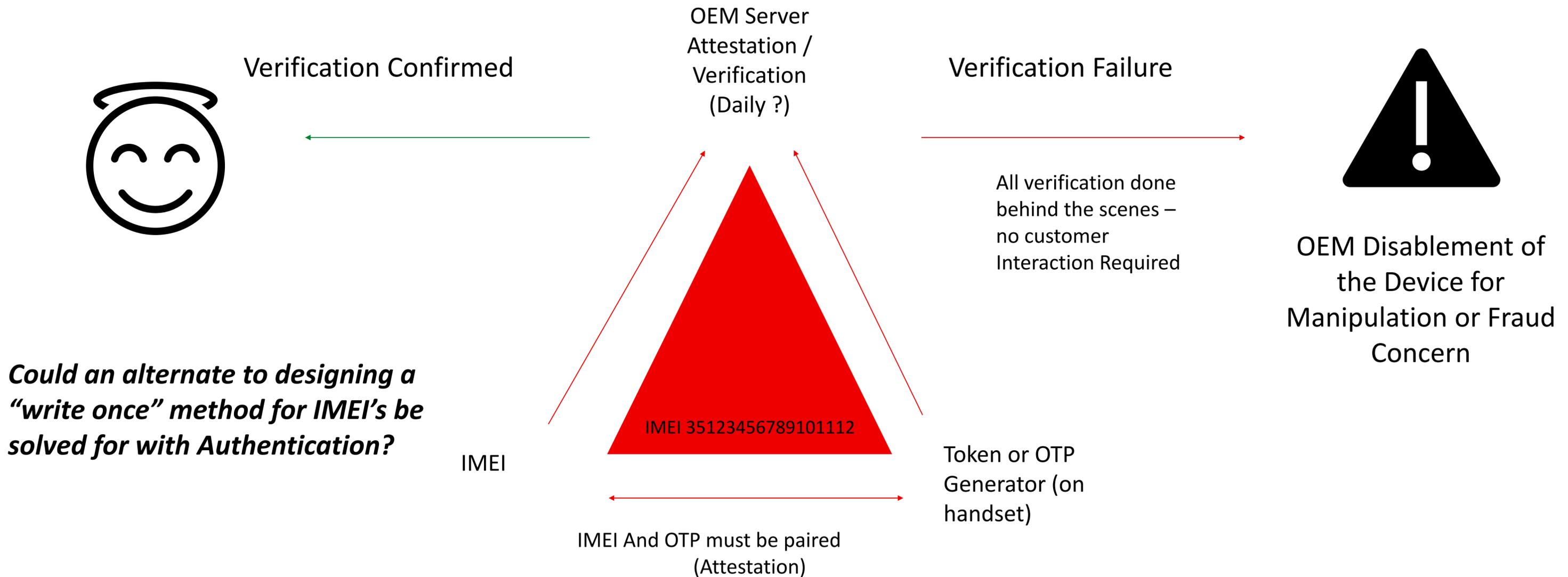


Making it harder to hide the identity of a device will make it easier to prosecute criminals



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:



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



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:

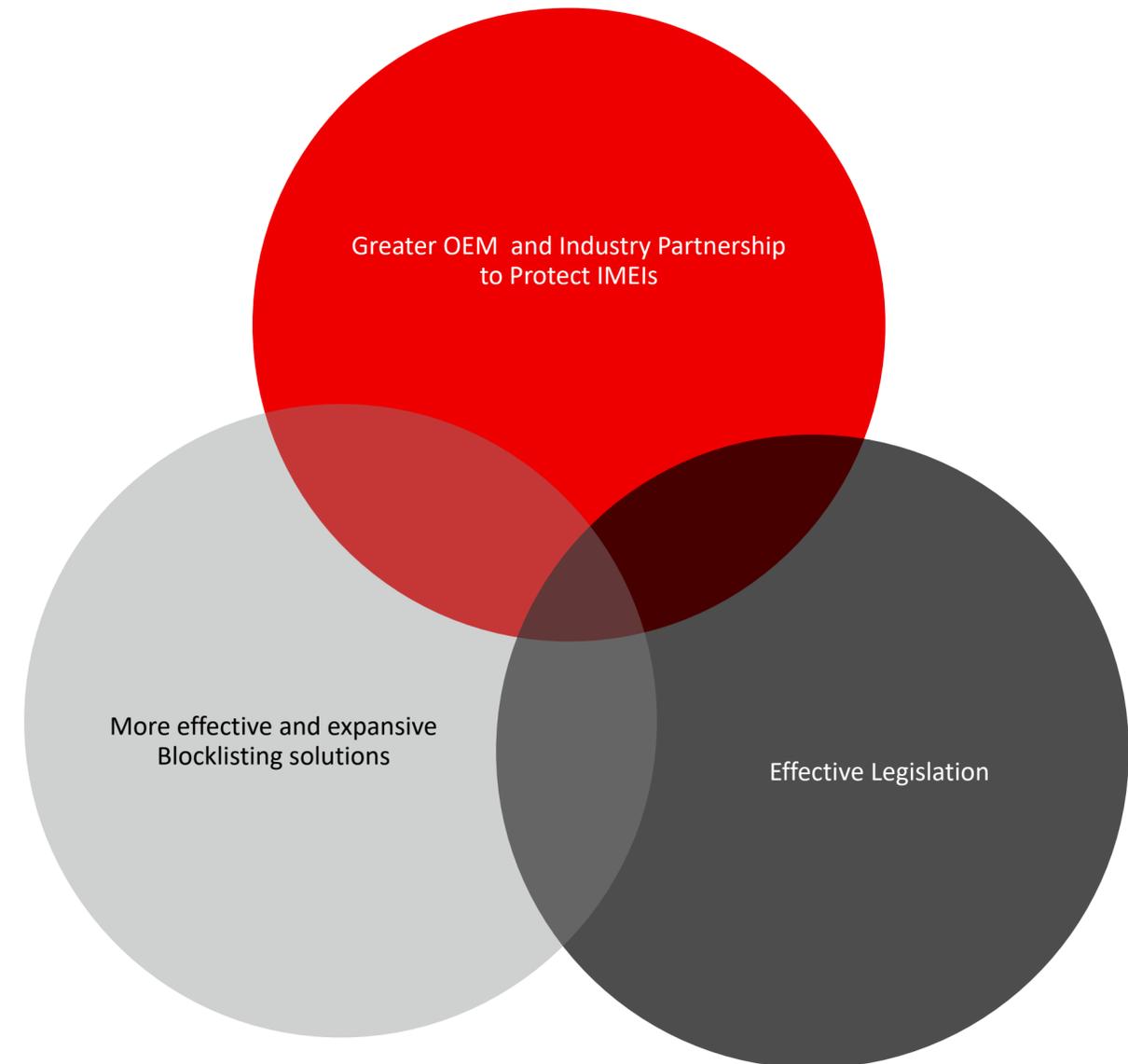
- Multiple delays due to COVID and COVID related legislative efforts
- Varying definitions of Fraud from Country to Country
- Stalemate with Right to Repair Lobbyists



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?**