GSMA Block List Services Description

for GSMA Block List Contributors and Users

Effective Date: 14 January 2021

This document sets out the services description and data management considerations for users of and contributors to the GSMA Block Lists[1] via platforms including GSMA Device Registry, GSMA Device Check, Stolen Phone Checker, and IMEI DB (**Block List Services**)[2].

Contents

Role of GSMA and IMEI

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

The GSMA is also the global custodian for the global TAC/IMEI system. The IMEI is a 15-digit number implemented by a device manufacturer which acts as a unique device identifier for 3GPP mobile devices, such as feature phones, smart phones, laptop dongles, and cellular IoT modems.

As part of the GSMA's work to combat mobile device fraud and theft, GSMA operates the GSMA Block Lists and the Block List Services. GSMA Block Lists are databases of information about lost, stolen, faulty, broken and fraudulently obtained mobile devices.

Introduction to the GSMA Block Lists

The GSMA Device Block Lists help to flag devices that are not with their rightful owner or are otherwise unsuitable for use on cellular networks, by placing them on a "block list". The GSMA maintains a global Block List consisting of devices reported from many sources:

- Participating mobile network operators, known as Contributor Network Operators (**CNOs**) contribute device data to the GSMA Block List. CNOs often also use data from others to manage their own block list as a means to prevent or block devices from using mobile networks.

[1] Previously known as the "GSMA Black Lists".
[2] Previously known as the "GSMA Black List Services".

- Other GSMA approved organizations who manufacture, insure or trade mobile devices contribute device data as well and are referred to as Contributor Third Parties (**CTPs**).

Collectively, CNOs and CTPs are referred to as “Contributors”. When the Contributor name is displayed in the Block List Services, CTPs are distinguished from CNOs by including “CTP: “in front of the organization name in the relevant record. See below for more information on Contributors.

Access to GSMA Block List Information

Qualified entities who meet GSMA’s requirements[3] are eligible to access and use the GSMA Block List information via the GSMA Block List Services. User access is via:

- **For Stolen Phone Checker and GSMA Device Check Users**: Users must submit a device identifier (IMEI, MEID or ESN) via API or web interface, to query the GSMA Block List.

- **For Contributor Network Operators (via IMEI DB or Device Registry):** Users may submit a device identifier (IMEI, MEID or ESN) via web interface to query the Block Lists, or may receive Block List information via Secure FTP file download.

These services help users to query the status of a device to know if it is suitable for sale or use on cellular networks.

Varying levels of GSMA Block List information are available to certain user types. The GSMA Mobile Device Crime Data User Access Policy (as updated from time to time) defines who may access GSMA Block List information, what fields of information each type of user may receive, and how each user may receive and use the GSMA Block List information[4]. The general public is only permitted to view whether a device is on the Block List whereas commercial, law enforcement and government organizations are additionally permitted to view Contributor name and transaction date of each entry. Individuals should contact their Mobile Network Operator with further queries if their mobile device is listed on the GSMA Block List Services.

GSMA-approved CNO users may also view GSMA TAC (mobile device model) information relating to the GSMA Block List records.

Description of GSMA Block List Information

The GSMA Block Lists are capable of capturing the following data fields, though depending on the nature of the contributor or user, not all fields will be available:

- Mobile device IMEI (or MEID or ESN)
- Date of the GSMA Block List entry
- Country and Contributor responsible for the entry
- Device make and model detail (TAC information) associated with the IMEI
- Reason Code (see table in Appendix)
- History of Block List entries

If an IMEI (or MEID or ESN) has not been reported by a Contributor, no data relating to that IMEI is contained in the GSMA Block Lists.

Depending on the user/product type, only certain information from the GSMA Block Lists is collected and disclosed[5].

No device owner information (e.g. name, telephone number, or other such information) is reported or held in the GSMA Block Lists. However, as further discussed below, GSMA considers that both the

[3] Including without limitation: (i) Mobile Device Crime Data User Access Policy requirements, as updated by GSMA’s working groups from time to time; and (ii) GSMA’s customer due diligence and compliance requirements.

[4] For Contributor Network Operators, the *SG.18 Device Registry Specification and Access Policy* applies instead.

[5] Access requirements are further set out in the Mobile Device Crime Data User Access Policy.

device identifier and associated GSMA Block List information may in some circumstances be considered personal data or personally identifiable information for regulatory purposes.

Submissions to the GSMA Block List

GSMA Block List information is reported directly to the GSMA Block Lists by participating mobile network operators and other entities approved by GSMA. GSMA provides the reporting platforms and specifies the file format for exchange of Block List information but does not submit, verify or vet information, which is solely submitted by Contributors. GSMA and Contributors therefore disclaim responsibility for the accuracy, currency or completeness of the GSMA Block List data.

GSMA Block List Data Contributors

Block List information is contributed by the following:

- **Contributor Network Operator (CNO)** is a GSMA-approved mobile network operator (MNO) with the intent and ability to block devices on its network and to upload IMEI records to the GSMA Device Registry for the purpose of combatting device theft and fraud. Prospective CNOs can apply to participate by contacting GSMA at https://imeidb.gsma.com..

- **Contributor Third Party (CTP)** is a GSMA-approved organization who manufactures, insures or trades mobile devices, and has the intent and ability to upload IMEI records to the GSMA Device Registry for the purpose of combatting device theft and fraud. Prospective CTPs can apply to participate by contacting GSMA at https://imeidb.gsma.com.

With the exception of the general public, Contributor names are available to users of the Block List Services. Some Block List Services APIs and web interfaces provide Device History that lists the Contributor name and transaction date. Users of the Block List Services are prohibited from disclosing the Contributor name to the general public.

CTPs are distinguished from CNOs by using the pre-fix “CTP:” before the Contributor name. Users of the Block List Services are prohibited from disclosing the Contributor name to the general public.

Contributors’ contact information is stored by GSMA and is available (i) to CNOs via their Block List access platform; and (ii) to CTPs upon valid request to GSMA.

Query Logs

GSMA is not provided with, and does not store, any information about individual ownership or usage of a device. However, GSMA stores logs of which organizations query or download the Block List, including the device identifier, time of query, and, in the event of a public look up, the source IP address of the check. These query logs are used by GSMA for operational purposes and may also be disclosed to law enforcement users, but are not otherwise provided by GSMA to third parties.

Infrastructure and Storage

The GSMA Block Lists and Block List Services are operated by GSMA Ltd, a wholly owned subsidiary of the GSM Association with an office at 165 Ottley Drive, Suite 150, Atlanta, Georgia, 30324, USA. The Services are supported and maintained by GSMA’s ISO 27001-accredited partners based outside of the EEA, subject to the Model Processing Clauses. The infrastructure supporting the GSMA Block Lists and Block List Services is on Amazon Web Services (AWS) in the U.S., being certified under the EU-US Privacy Shield.

GSMA Block List data is stored in perpetuity, because once a device is lost or stolen this status has no expiry date and remains relevant to the ecosystem. In the event that a lost or stolen device is found, the fact that the device had temporarily been lost remains relevant to the ecosystem in the event of dispute resolution and/or criminal investigation.

Personal Data Regulation

The General Data Protection Regulation (**GDPR**) (EU) 2016/679 is in force as of 25 May 2018. Under the GDPR, "personal data" includes any information that can be used to directly or indirectly identify a natural person. A mobile device is generally used by a single individual and therefore a device identifier such as an IMEI could be used by some entities to link to or identify a specific individual.

Although GSMA is not handling personal data associated with devices, in the context of increasingly broad global data regulation, GSMA considers it prudent to treat device identity data such as IMEI and GSMA Block List information in a manner consistent with personal data.

To the extent that the GSMA Block Lists and Block List Services may involve processing of personal data under the GDPR, in all cases, GSMA, Contributors and data users each process the personal data on their own behalf, and for their own purposes (subject to the permitted data uses set out the in the relevant legal agreements and GSMA policies[6] (as applicable). For GDPR purposes, GSMA considers that each entity participating in the GSMA Block List Services is therefore a "data controller"[7] in its own right.

The GDPR applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location. Because GSMA maintains an establishment within the EU, and because the GSMA Block Lists contain information which may relate to EU data subjects, GSMA considers that GDPR requirements are relevant to all contributors and users of the GSMA Block Lists, regardless of their location.

Accordingly, you and GSMA shall treat IMEI-related information exchanged through the GSMA Block List Services as "personal data" for the purposes of data protection regulation. As part of this commitment, each of GSMA and you shall:

- comply with relevant data protection laws in its role as an independent Data Controller, including the requirements of the General Data Protection Regulation (GDPR) (EU) 2016/679;
- use reasonable commercial endeavours to prevent unauthorised access to or manipulation of the GSMA Block List information;
- limit access of data to authorised personnel on a need-to-know basis; and
- promptly notify the other in the event of any relevant data breach.

Where you are outside the European Economic Area, United Kingdom or Switzerland[8], the transfer of any IMEI-related information from GSMA to you or vice versa shall be subject to the Standard Contractual Clauses[9].

Disclaimer

This document is intended for general information purposes only and is not intended as legal advice. By its nature, this document is necessarily a summary only, and cannot be taken as comprehensive. Specialist advice should be taken in relation to your specific circumstances.

Although GSMA endeavours to ensure that this document is correct, no warranty, express or implied, is given as to its accuracy and we do not accept any liability for error or omission. GSMA shall not be liable for any loss, damage or liability (howsoever caused) arising from the use of, or inability to use, this document or any material contained in it, or from any action or decision taken as a result of using this document.

[6] SG.18 Device Registry Specification and Access Policy, FS.44 Mobile Device Crime Data User Access Policy, and FS.45 Device Blocking and Data Sharing Recommendation.

[7] "controller" in Article 4 (7) the General Data Protection Regulation (EU) 2016/679 (GDPR), being a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

[8] Save for where you are in a third country which is subject to an adequacy decision by the European Commission.

[9] *Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)* (Set II) as set out in the Annex to *Commission Decision 2004/915/EC, incorporated herein by reference.*

This document is current as of 14 January 2021, and summarizes applicable GSMA policies as at this date. This document and the relevant policies may change from time to time without notice.

Updates

GSMA may update this Service Description and the relevant GSMA Policies referenced herein from time to time, by updating this document at https://devicecheck.gsma.com/deviceregistryservices. GSMA will act reasonably to notify GSMA Device Check and Stolen Phone Checker users of any updates by email notification. Your continued use of the Block List Services or Block List information following the update constitutes your acceptance of the updates.

Contact Us

For more information on the GSMA Block List Services or other GSMA programs to combat mobile device theft and fraud, please contact devicecheck@gsma.com.

Appendix – Summary of Block List Reason Codes

Code	Value	Direction	Usage
0010	Faulty or Broken	Insert	Equipment suspected to be faulty or broken.
0018	Repaired	Remove	Equipment deemed available for use after having been previously identified as Faulty or Broken.
0011	Stolen or Lost	Insert	Equipment identified as stolen or lost.
0014	Found	Remove	Equipment identified as found after having been previously identified as Stolen or Lost.
0026	Fraudulently obtained	Insert	CNO use only. Equipment identified as fraudulently obtained from Operator with sufficient evidence that a police complaint could be filed.
0027	Validly obtained	Remove	CNO use only. Equipment identified as having been validly obtained.
0016	Duplicated IMEI	Insert	IMEI identified as copied into multiple devices.
0020	Unique IMEI	Remove	IMEI determined to be unique after having previously been identified as a duplicate.
0023	Third party request to add	Insert	CNO use only. IMEI submitted by Operator to the Block List in response to request by a third party (e.g. law enforcement, retail store).
0024	Third party request to remove	Remove	CNO use only. IMEI removed from the Block List by Operator when previously added in response to request by a third party.
0028	Court ordered block[10]	Insert	CNO use only. IMEI blocked in response to a Court Order, issued from a competent court that requires a CNO to block an IMEI e.g. court order to block a device used illegally in correctional facilities (aka "Contraband").
0029	Court ordered unblock[11]	Remove	CNO use only. IMEI unblocked in response to a Court Order, issued from a competent court that compels or allows a CNO to unblock an IMEI that was previously compelled to block.
0022	Aged IMEI	Remove	System level record used only to identify to Operators that a certain time period has passed since the device was added to Block List. *May also be used by Operators to remove records due to the passage of time.*

Please note that not all reason codes are available to all users of the Block List Services.

For more detailed information on the GSMA Block List technical specifications, please refer to *GSMA Permanent Reference Document SG.18 - Device Registry Specification and Access Policy*.

[10] Approved under policy but not yet operationally implemented as at the release date of this document.
[11] Approved under policy but not yet operationally implemented as at the release date of this document.