New Zealand Telecommunications Forum

Code for Blocking Blacklisted Mobile Handsets between Mobile Operators

("IMEI Blacklisting Code")

Code Status:	**Endorsed**
Code Classification:	Voluntary Code
Date:	May 2019 (3rd edition)
Review Status:	This Code was reviewed by the Working Party in 2019. It was determined that no amendments were necessary. The next review is due in 2021.

TABLE OF CONTENTS

A Defined Terms

Agent	refers to an entity or Person with the authority to sell Handsets and Telecommunications Services on behalf of an Operator
Blacklist	refers to an IMEI that has been blocked by an Operator in their EIR and uploaded to the IMEI Database for blocking in other EIRs, in accordance with agreed Blacklisting policies
Business Day	means a day on which registered banks are open for normal banking business, excluding Saturdays, Sundays and nation-wide public holidays. Regional public holidays are considered to be Business Days.
CCF or Code Compliance Framework	means the TCF's Code Compliance Framework as endorsed by the TCF Board and being the overarching compliance and enforcement regime for TCF codes.
Clause	refers to a clause in this Code
Code	means this IMEI Blacklisting Code
Code Signatory(s)	refers to an Operator that has signed up to this Code
Commencement Date	is the date set out in clause 6.1
Compliance Officer	means the person appointed by the TCF as the compliance officer under the Code Compliance Framework
Customer Service	refers to all Subscriber facing staff that have the authority to Blacklist a Handset on behalf of a Subscriber
Duplicate IMEI	means an IMEI that an Operator has recorded as being in use in two or more different locations at the same time.
Equipment Identity Register (EIR)	means the register required by Operators to enforce the Blacklisting of IMEIs on their cellular network
Fraud or Fraudulent	Has the meaning set out in clause 11.2.
GSM Association (GSMA)	means the international association of GSM mobile operators
Handset(s)	means a device used for cellular mobile communications, this includes devices that have a data only capability
Insurance Company	means an insurer with a 'handset replacement policy' that has a formal relationship with an Operator for the blacklisting of Handsets under those policies.
International mobile equipment identity (IMEI)	means an international 15 digit identifier applied physically and logically within cellular Handsets, made up of a unique 14 digit identifying sequence and a single 15th "check" digit.
IMEI Database	means the database maintained by the GSM Association to facilitate the sharing of lost, stolen and Fraudulently obtained IMEIs between Operators
IMEI Data	means the first 14 digits of an IMEI and the "reason codes" that are exchanged between Operators for Blacklisting and Un-Blacklisting
IMSI	means an International Mobile Subscriber Identity, used by Operators to identify a Subscriber on their network.
Mobile Virtual Network Operator (MVNO)	means an operator selling cellular mobile telephony and communication services on a network Operator

MSISDN	means a Mobile Subscriber Integrated Services Digital Network number, used by an Operator, to identify a Subscriber on their Network.
Non-consumer Subscriber	means either a corporate and government subscriber or a business subscriber of an Operator which has multiple connections associated with their Operator
Operator	means a party operating a radio-frequency cellular network in New Zealand who has signed up to this Code.
Person	means a legal person and includes a company and any other legal entity.
Reason Codes	means those numeric codes set out in Schedule 2 of this Code used to identify the reasons why an IMEI has been added or removed from the IMEI Database.
Subscriber	means the account-holder or a person with authority on the account-holder's behalf, or, in the case of "prepay" services, the customer
TCF	means the New Zealand Telecommunications Forum Incorporated
Un-Blacklisting	mean the unblocking of a Handset IMEI by an Operator allowing the Handset to be used on its network, and uploaded the IMEI Database so it can be used on other Operator's networks.

B Introduction

1 Background

1.1 Mobile Handset theft is an increasingly common problem in New Zealand.

1.2 Each Operator in New Zealand has now individually invested in an Equipment Identity Register (EIR) for their cellular network which provides the capability to block or "blacklist" Handsets from using their network.

1.3 Handset blacklisting occurs by reference to the 15 digit identifier, the International Mobile Equipment Identity (IMEI), attached to each device worldwide. This identifier is administered by the GSM Association for Handset manufacturers and operators globally. The IMEI is normally imprinted physically and logically within a Handset. Operators can use their EIR to decide whether an IMEI should attach to their network or not.

1.4 Operators blacklist Handsets on their networks for a variety of reasons including:

a) to assist subscribers who have had their Handset lost or stolen, or

b) to prevent fraudulently acquired devices, or devices stolen from an Operator, from attaching to their network.

1.5 Prior to the Code, blacklisted Handset IMEIs were shared on an ad-hoc basis between Operators with no systematic coordination for New Zealand Operator-wide blacklisting The limited sharing of IMEIs contributed to opportunistic behaviour where Handsets blacklisted by one Operator were then able to be used on the network of another Operator.

1.6 An industry blacklisting database has been successfully adopted in other markets such as Australia and the United Kingdom through the cooperation of Operators.

1.7 Industry blacklisting will deter the incentives for Handset criminal activity in New Zealand.

2 Purpose

2.1 The purpose of this Code is to establish coordinated sharing of IMEIs between mobile networks in New Zealand to discourage the theft and fraudulent acquisition of mobile Handsets, and to disrupt the operation of illegal markets dependant on such activity.

3 Scope

3.1 This Code sets out the terms for sharing Blacklisted IMEIs between Operators in New Zealand, that have been blocked by one Operator for a matter prescribed within the Code.

3.2 This Code also covers the sharing of Un-Blacklisted IMEIs.

3.3 Un-Blacklisting is an important part of the customer experience enabling a customer to reuse their Handset and legitimately move their service between Operators and to and from MVNOs.

4 Objectives

4.1 The objectives of this Code are to:

(a) Facilitate the timely sharing of agreed Blacklisted/Un-Blacklisted Handsets between New Zealand Operators.

(b) Specify a common information technology framework that Operators will use to share Blacklisted and Un-Blacklisted IMEIs.

(c) Govern the terms when Blacklisted and Un-Blacklisted IMEIs are shared. This common policy framework is crucial to providing a consistent message to industry and end-users.

4.2 Scope exclusions

4.2.1 This Code does not apply to MVNOs unless an Operator grants an MVNO access to their EIR to Blacklist and Un-Blacklist IMEIs. The TCF may agree to extend the operation of the scheme to all MVNOs in the future and will consult on the necessary extensions and amendments to this Code at that time.

4.2.2 The Code and scheme does not apply to other "blacklisting" services Operators may offer for their customers relating to their MSISDN or IMSI etc.

4.2.3 The Code does not apply to any IMEI blacklisted by international operators, until it has been agreed by the Operators to extend the scheme to international IMEIs.

5 Principles

5.1 This Code will facilitate ongoing coordinated sharing of Blacklisted IMEIs between New Zealand Operators and will be used to facilitate any new Operator into the sharing arrangement.

5.2 IMEI sharing will only occur in accordance with the agreed Handset Blacklisting policies, set out in this Code.

5.3 Operators shall not Blacklist or un-Blacklist an IMEI in order to gain any commercial advantage or inflict any damage on any other Operator or party. Blacklisting cannot be used to withhold service or resolve commercial disputes (including bad debt scenarios). Operators cannot use any contact made by a former customer requesting to Un-Blacklist an IMEI for any "win back" or sales activity.

5.4 Only:

a) a Subscriber;

b) an authorised representative of a Non-consumer Subscriber;

c) an Operator itself in relation to an Operator owned Handset(s) or Fraudulent IMEIs; or,

d) an Insurance Company on behalf of a Subscriber

can request that an IMEI be Blacklisted. Other third parties, including law enforcement, are not able to request that an IMEI be blacklisted, unless blacklisting is required by any warrant, court order or by any law.

5.5 Only the Operator who has either a relationship with:

(a) The Subscriber, or Non-consumer Subscriber, whose Handset has been lost or stolen; or,

(b) Directly with the Handset (IMEI) in question,

is permitted to undertake Blacklisting. Updating new entries for Blacklisting and Un-blacklisting will occur within the agreed timeframes set out in this Code.

5.6 If an MVNO Blacklists or Un-Blacklists an IMEI directly through an Operator's EIR, that MVNO will be responsible for ensuring that it adheres to the terms of this Code. Operators must ensure that any MVNO of theirs that they permit to access their EIR is aware of and agrees to abide by the terms of this Code. Where an Operator Blacklists an IMEI on behalf of an MVNO, the Operator will be responsible for ensuring that the MVNO has complied with any relevant requirements of this Code.

5.7 In the future, Operators may, in consultation with other relevant parties, agree to leverage the capability of the IMEI Database to expand their IMEI Blacklisting to include the blocking of IMEIs

from other jurisdictions that also use the GSMA database capability. Any agreement will be reflected in an amendment to this Code.

6 Commencement and Compliance

6.1 This Code shall come into force on the later of:

a) the date it is endorsed by the TCF Board; or,

b) the date that the three original Operators (Telecom New Zealand, Vodafone New Zealand and 2Degrees Mobile) confirm that their inter-carrier testing is complete and they are ready to make Blacklisting live.

6.2 The TCF Code Compliance Framework (CCF) applies to the ongoing monitoring and compliance of this Code. By becoming a Code Signatory, Code Signatories agree to comply with and are bound by the terms of the CCF in relation to the performance of their obligations under this Code.

6.3 For the purposes of the self-certification requirements under the CCF, the key metrics of this Code that Code Signatories are required to self-certify they comply with are set out in Schedule 1.

6.4 Parties that sign up to this Code after it comes into force must have an EIR and will have 3 months from the date of signing to make any necessary changes to comply with the requirements of the Code.

6.5 The CCF's complaints management procedures will apply to any allegations of a breach of this Code, made by one Code Signatory about another to the Compliance Officer. By signing up to this Code, Code Signatories agree to abide by the terms of the CCF and will cooperate in a full and frank manner with the Compliance Officer at all times, participate in good faith in any investigations they may be involved in and adhere to any sanctions levied against them under the CCF in relation to this Code.

6.6 In the event of any inconsistency between this Code, any relevant legislation, and any relevant GSMA policies and requirements, this inconsistency will be resolved in the following (descending) order of precedence:

a) Any legislation;

b) The GSMA policies and requirements

c) This Code.

6.7 This Code contains the minimum requirements regarding the blacklisting of IMEIs between Operators. Operators may agree to adhere to a higher standard as part of any bilateral agreement reached between themselves from time to time.

7 GSM Association Database and Expectations

7.1 Code signatories agree to use the IMEI Database operated and maintained by the GSMA for facilitating the exchange of agreed categories of Blacklisted IMEIs, and the Un-Blacklisting of such IMEIs. The IMEI Database will be accessible to Operators through arrangements made directly with the GSMA.

7.2 Each Operator will abide by the GSMA Guidelines for using its IMEI Database.

7.3 Operators recognise that nothing in this Code shall affect the authority of the GSMA to manage the IMEI Database in accordance with its own systems, policies and processes, including an ability to suspend or alter access to the IMEI Database from time to time.

7.4 Each Operator must be a GSMA member to access the IMEI Database, which is provided free of charge to GSMA members.

7.5 Operators recognise that the GSMA will maintain appropriate and sufficient technical and organisational measures to protect Operator IMEI data against accidental or unlawful destruction,

loss, damage, alteration, or unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing. The GSMA will at all times hold and process Operator IMEI data only for the purpose of operating the IMEI Database.

8 Operators EIR Implementation

8.1 Operators will operate their own EIR enabling them to block IMEIs in their network.

8.2 Operators will add Blacklisted IMEIs downloaded from the IMEI Database to their own EIRs unless it is reasonably believes that:

a) an error has been made;

b) the IMEI was entered with malicious intent; or,

c) duplication is suspected.

8.3 Operators will add Blacklisted IMEIs on their EIR within two working days of being notified of the IMEIs that have been placed on the IMEI Database, in order to minimise risk of theft and resale of the devices

8.4 Operators will remove IMEIs from their EIR blacklist within one working day of being notified by the IMEI Database of an IMEI's removal from the IMEI Database

8.5 Operators may maintain historical lists of IMEIs that they know should remain active on their network, and may use these lists to avoid blacklisting where an IMEI is known to be a Duplicate IMEI. Operators may upload these "greylists" to the GSMA database if they wish for other parties to retrieve them as required, or the lists may be shared directly by agreement with other parties.

9 Managing the IMEI Blacklist – Blacklisting and Un-Blacklisting

Handset Blacklisting

9.1 The Operator will ensure that it has appropriate policies in place to ensure that only authorised users can add or remove items from the IMEI Database. The Operator must be able to show that it has the appropriate aforementioned processes in place if required to resolve a Compliance Issue.

9.2 A Subscriber is deemed to own a Handset (Handset Owner) if:

a) they can show that they lawfully obtained the Handset (whether from an Operator or another person);

b) the Operator and/or the Subscriber can reasonably show that they had control and/or possession of the Handset prior to it being lost or stolen; or,

c) The Operator can check and verify that the IMEI has been used by that Subscriber.

9.3 Notwithstanding clause 9.2a), if a person purchases a Handset from another person other than an Operator (particularly a second hand handset) it is incumbent on that person to make all possible inquiries to ensure that the Handset has not been lost, stolen or fraudulently acquired. Acquiring a lost, stolen or fraudulent Handset through a lawful transaction will not be sufficient evidence for the person to be deemed a Subscriber for the purposes of this Code.

9.4 If an Operator is unable to verify that an IMEI has been used by the Subscriber then the Operator must decline to Blacklist that IMEI.

9.5 An Operator owns a Handset when the Handset has been stolen from the Operator or from an Agent of the Operator, or when the Handset was acquired on Fraudulent terms from the Operator or from an Agent of the Operator.

What Should be Blacklisted

9.6 Only those IMEIs identified as lost or stolen by a Subscriber (including through an Insurance Company), or identified directly by the Operator as fraudulent under clause 11, shall be added to the IMEI Database.

9.7 Due to the risks caused by historic data, IMEIs blacklisted by an Operator prior to Commencement Date can continue to be blacklisted on that Operator's own network but cannot be added to the IMEI Database.

9.8 The Operator must only add the IMEI Data and such other data required by the GSMA file formatting requirements, using a prescribed Reason Code set out in Schedule 2, to the IMEI Database. Identifiable personal data related to Subscribers shall not be supplied to the IMEI Database or exchanged by the Operators.

9.9 If an Insurance Company requests an IMEI be Blacklisted, the Operator will ensure that the relevant Reason Code is added to ensure the record also notes the action was undertaken at the insurer's request.

9.10 The Operator must ensure that it has processes in place to ensure the integrity of the information that is to be inputted to the IMEI Database and Operators should always check the accuracy of the information supplied by their Subscribers prior to any posting.

9.11 The decision to Blacklist and/or Un-Blacklist a device shall not be made in order to gain commercial advantage or inflict damage to any other Operator or party and should not be used to withhold service or to resolve commercial disputes.

9.12 The Operator must update the IMEI Data as soon as practicable if they discover that the Reason Code associated with the Blacklisted IMEI changes, is incorrect or is misleading.

IMEI Sharing

9.13 Each Operator must build and maintain its file-transfer process to the GSMA IMEI Database in accordance with the GSMA's SG.18 IMEI Database File Format Specification (record format 2), unless otherwise agreed between Operators and the GSMA. Each Operator must comply with any relevant changes prescribed by the GSMA for the file-transfer process.

9.14 Each Code signatory will agree to exchange Blacklisted and Un-Blacklisted IMEIs in accordance with the policies in this Code on a daily basis. As far as it is possible, Blacklist entries shall be submitted to the IMEI Database on a daily basis between 22:00 and 00:00 and updated lists from other Operators will be downloaded as soon as practicable thereafter, usually around 04:00 the next day.

C Handset Blacklisting and Un-Blacklisting policies

10 Subscriber Originated Handset Blacklisting: lost and/or stolen Handsets

10.1 Subscriber initiated Blacklisting for lost or stolen Handsets can only be initiated by the Handset owner as defined in clause 9.2.

10.2 For Non-consumer subscribers, a designated user of the Handset or a duly authorised representative of the Non-consumer subscriber may request a subscriber blacklisting for a lost or stolen Handset.

10.3 Before initiating any action to Blacklist a subscriber originated lost or stolen Handset, the Operator must verify the identity of the Subscriber in accordance with their standard authorisation and security processes. Where an Insurance Company requests the Blacklisting, the Operator will be responsible for ensuring that those entities undertake the necessary verification of the Subscriber.

10.4 Operators must also record sufficient alternative contact information for Subscribers initiating a Handset Blacklisting.

10.5 The TCF may, in consultation with Operators, implement additional policies and guidelines as required from time to time regarding any timeframes or "long stop" period in which Subscribers can initiate Blacklisting with an Operator for lost/stolen Handsets. Operators will be required to adhere to any such policies as if they formed part of this Code.

11 Operator Originated Handset Blacklisting: Fraud, lost or stolen

11.1 Operator originated Handset Blacklisting must only occur for:

- Handsets stolen from an Operator or their Agent. In this case, the "lost/stolen" Reason Code can be used; or,
- Fraudulent activity perpetrated by a Subscriber, or someone purporting to be a current or potential Subscriber, on the Operator's network. Where it is deemed that Fraud or Fraudulent activity has occurred the Operator should use the "Fraud" Reason Code.

11.2 "Fraud" or "Fraudulent" activity is activity undertaken in apparent contravention of section 240 of the Crimes Act 1961, that is, by a person(s) using deception, without claim of right, to obtain ownership, possession or control over any device with an IMEI. Deception means a false representation, whether oral, documentary or by conduct, where the person making the representation intends to deceive any other person and knows that it is false in a material particular.

11.3 Before an IMEI can be added to the IMEI Database under the category of Fraud a case must satisfy the burden of proof and the following must apply:

a) There must be documentary and/or other evidence which prima facie supports the allegation of fraud; and,

b) There must be sufficient evidence to lay a Police complaint, though Code Signatories may choose when they will or won't lay a Police complaint.

11.4 The TCF may, in consultation with Operators, implement additional policies and guidelines as required from time to time regarding any timeframes or "long stop" period in which Operators can initiate Blacklisting for Fraudulent activity. Operators will be required to adhere to any such policies as if they formed part of this Code.

12 Un-Blacklisting

12.1 Due to how blacklisting operates through the IMEI Database, Un-Blacklisting of IMEIs can only be performed by the Operator responsible for the original Blacklisting of the Handset. If a Subscriber has since moved to an alternate provider, they must contact the original Blacklisting Operator to have the Handset Un-Blacklisted.

12.2 Operators cannot use any enquiry about an IMEI for any "win back", promotional, marketing or sales related activity.

12.3 An IMEI cannot be Un-Blacklisted at a Subscriber's request unless the Operator is satisfied that an error was made at the time the IMEI was Blacklisted, or if the Reason Code associated with the IMEI was "lost/stolen" and the Operator is reasonably satisfied by the Subscriber that the Handset has now been found or recovered.

12.4 Notwithstanding clause 12.3, an Operator will not Un-Blacklist an IMEI where the IMEI Database records a Reason Code noting the involvement of an Insurance Company, without first obtaining the approval of the relevant Insurance Company. This is to reduce the occurrences of insurance Fraud.

12.5 Only the original Subscriber that requested the Blacklisting may request that an IMEI be Un-Blacklisted. The Operator must take all reasonable steps in accordance with its own security policies to verify the identity of the Subscriber before Un-Blacklisting the IMEI.

12.6 For a Non-consumer Subscriber, a request for Un-Blacklisting may only be initiated by an authorised person on the account.

12.7 The Operator will remove the IMEI from its blacklist as soon as it is aware that the reason code used to add the IMEI to the blacklist is no longer valid. The Operator will submit the IMEI with the corresponding Un-Blacklist Code set out in Schedule 2 to the IMEI Database as soon as practicable to complete the Un-Blacklisting process.

13 Incorrect Blacklisting

13.1 Where an incorrectly Blacklisted IMEI results in another Operator's subscriber having their Handset blacklisted, that Operator may Un-Blacklist their Subscriber's IMEI in their own EIR, provided they have taken reasonable steps to confirm that the Handset had been erroneously blacklisted.

13.2 Before an Operator can Un-Blacklist an IMEI that was incorrectly Blacklisted, it must be satisfied the Subscriber's Handset is not the subject of:

a) a confirmed case of Fraud by another Operator under clause 11, which can be corroborated by contacting the relevant Operator; or,

b) a lost or stolen claim, which can be corroborated by evidence such as (but not limited to):

i. The IMSI is in use but the Handset has not changed for a period of at least 3 months and the subscriber and Operator can verify this (including up to the date when the IMEI was blacklisted);

ii. The 3 month call record for the subscriber does not indicate there has been a change with the MSISDN (including up to the date when the IMEI was blacklisted); or,

iii. The IMEI belongs to an on-account subscriber and the IMEI that has been recorded with the Operator, or the IMEI belongs to a Non-Consumer Subscriber and their IMEI is recorded with the Operator.

13.3 The effected Operator must contact the Operator responsible for the Blacklisting of the IMEI to notify of the blacklisting error. The blacklisting Operator should then verify if there was an error involved with the blacklisting

13.4 Where both Operators are satisfied the processes in clause 13.2 have been correctly followed they will ensure the IMEI Database reflects the correct status of the IMEI.

13.5 Operators must keep an auditable list of the IMEIs it has Un-Blacklisted.

D IMEI sharing file transfer processes

14 Service outages

14.1 An Operator must notify other Operators by email of instances when it has failed to complete its daily file exchange process and cannot rectify it in the following day's file exchange.

14.2 If the Operator has not been able to participate in the daily file exchange process for 7 days it should cease daily notifications and must notify other Operators that it cannot participate in the daily file exchange process. As part of this notification it must:

a) Specify the cause for the outage.

b) The expected time involved with correcting the issues involved with the outage and

c) Whether a manual-work around solution can be implemented during the outage.

14.3 The Code signatory must also notify other signatories when its file exchange process has recommenced, and whether its EIR has successfully populated Blacklisted and Un-Blacklisted IMEIs transferred by other signatories to the GSMA IMEI Database

14.4 In the event of any continued difficulty in accessing the IMEI Database, an Operator may transmit its Blacklist to the other Operators directly by agreement.

14.5 If a technical or administrative failure prevents an Operator from Blacklisting or Un-Blacklisting another Operator/s IMEIs, that Operator must Blacklist or Un-Blacklist (as the case may be) the missed IMEIs as soon as possible. In such cases, any 'long stop' period does not apply.

15 Reporting

15.1 Code Signatories will leverage the functionality of the IMEI Database and their own EIR to produce quarterly volume totals of Blacklisted and Un-Blacklisted IMEIs (and any other reporting which may be agreed from time to time) that will be used by the Operators and the TCF to ensure that the Code is achieving its aims and objectives.

15.2 Public reporting of aggregated totals of Blacklisted and Un-Blacklisted quarterly volumes will be reported on the TCF website with the approval of the TCF Board.

15.3 Operators will report separately to the TCF on the number of IMEIs that could not be Blacklisted because they existed on an internal list in accordance with clause 8.5.

16 Third Party Access

16.1 Code signatories and the GSMA will work together to facilitate "read-only" access by the New Zealand Police to the IMEI database in accordance with the GSMA's policy for data visibility for law enforcement.

16.2 Code signatories and the GSMA will work together to facilitate "read only" access to the GSMA's database for other parties where such access is deemed appropriate.

17 Revocation and Amendment of the Code

17.1 In accordance with the TCF's Operating Procedures Manual, any TCF member may put a project proposal to the TCF Board (at any time) for the amendment or revocation of this Code. If you wish to propose changes to this Code, please contact info@tcf.org.nz

17.2 The TCF will undertake a review of this Code nine (9) months from the Commencement Date in order to assess the extent to which it is achieving its aims and objectives and any other relevant matter pertinent to the operation of this Code. Following this review, the TCF may undertake amendments to this Code as required, in accordance with the procedures set out in the TCF Rules and Handbook.

Schedule 1: CCF Self Certification Requirements

As part of the self-certification requirements of the CCF and this Code, parties must certify that they comply with the following clauses of the Code:

1 Clause 5.3 (Operators shall not Blacklist or un-Blacklist an IMEI in order to gain any commercial advantage or inflict any damage)
2 Clause 9 (Managing the IMEI Blacklist)
3 Clause 11 (Operator Originated Handset Blacklisting)
4 Clause 13 (Incorrect Blacklisting)
5 Clause 15 (reporting on volumes of Blacklisted and Un-Blacklisted numbers)

Parties must keep information they deem necessary to show their compliance with this Code, should it be required.

Schedule 2: Blacklisting and Un-Blacklisting Reason Codes

Operators will only use the following Reason Codes when adding or removing an IMEI to the IMEI Database.

(**NOTE**: the GSMA IMEI Database may use additional Reason Codes not listed here, a full explanation of all Reasons Codes can be found in the GSMA File Specification. Additional Reason Codes may be added to this Schedule 2 from time to time, with the agreement of the Operators and the GSMA.

Operators may use internal reason codes on their own EIRs which are not reflected in this list. Such codes are not supported by the IMEI Database).

Blacklisting Codes

CODE	REASON	USAGE	COMMENTS
0011	Stolen or Lost	Use when inserting an IMEI on the blacklist if the equipment has been identified as stolen or lost. This is NOT for use with a Duplicated IMEI	Can only be removed with reason code 14 & 22.
0016	Duplicated IMEI	Use when inserting an IMEI on the blacklists when the IMEI is known to be a Duplicated IMEI	Can only be removed with reason code 20 & 22.
0023	Third party request to add	Used when adding an IMEI to the blacklist at the request of a third party, ie an Insurance Company	Can only be removed with reason code 22 & 24.
0026	Fraudulent Use	Used to insert an IMEI on the Blacklist when Fraud has been found	

Un-Blacklisting Codes

CODE	REASON	USAGE	COMMENTS
0014	Found	Use when removing an IMEI from the blacklist if equipment previously designated as stolen/lost and has been found	
0020	Unique IMEI	Use when removing from the blacklist when the IMEI had been previously designated as Duplicated IMEI only	
0022	Aged IMEI	Not In Use by Operators at this time. May be used by Operators in the future if required to manually free up capacity on the IMEI Database or within Operator's EIRs.	This code is used for automatic ageing of IMEIs by the system. Can be used to remove IMEIs added to blacklists with reason code 10, 11, 16, 23 or 25.
0024	Third party request to remove	Used when removing an IMEI from the blacklist in response to a third party, ie an Insurance Company's, request	
0027		Used to remove an IMEI from the Blacklist if Fraud has subsequently be disproved or the matter successfully resolved.	

Quick Glance Table: Paired Blacklist/Un-Blacklist Codes:

Blacklist	Un-Blacklist
11	14, 22
16	20, 22
23	22, 24
26	27