A2P SMS Code of Conduct

Number and Status:	1.0 - Released
Date:	April 2018
Code Classification:	Self-regulated Code
Prepared by:	Mobile Ecosystem Forum (MEF) and MEF's Future of Messaging Programme participants
Notes:	This Code addresses Application-to-Person (A2P) SMS Services

TABLE OF CONTENTS

1 About the Mobile Ecosystem Forum

1.1 Established in 2000, The Mobile Ecosystem Forum (MEF) is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. MEF provides its members with a global and cross-sector platform for networking, collaboration and advancing industry solutions.

1.2 MEF's goal is to accelerate the growth of a sustainable mobile ecosystem that drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide.

2 About MEF's Future of Messaging Programme

2.1 Established in 2015, MEF's Future of Messaging Programme (the 'Programme') is a worldwide, cross-ecosystem approach to promote a competitive, fair and innovative market for mobile communication between businesses and consumers.

2.2 Programme participants represent different regions and stakeholder groups working collaboratively to:

- Reduce the number and impact of industry-wide Application-2-Person (A2P) fraud incidents
- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate enterprise messaging solution buyers about the threats and impacts of poor procurement processes with loose enterprise messaging requirements
- Build perceptions about enterprise messaging as a premium and trusted channel
- Facilitate innovation
- Promote new services and use cases
- Stimulate new partnerships

3 Trust in Enterprise Messaging

3.1 Part of the Programme, Trust in Enterprise Messaging ('TEM') is a self-regulation service and set of tools to build trust in enterprise messaging.

3.2 TEM's resources:

- A2P SMS Code of Conduct (the "Code")
- TEM Badge (the "Badge") – a digital logo, together with its associated compliance and respective terms and conditions of use, distributed by MEF to all Code signatories to be displayed and promoted across their digital platforms and marketing materials as a recognised symbol of best practice and trust.

4 The Code

4.1 The Code of Conduct ("Code") sets out a standard of behaviours, procedures and actions for all actors operating within the A2P SMS market (also referred to as enterprise, bulk or wholesale).

4.2 The Purpose of the Code is to establish a standard of behaviours, procedures and actions for all actors operating within the A2P SMS sector, in order to protect consumers, demonstrate ethical and commercial responsibility as well as to maximise value to all companies involved in the messaging ecosystem.

4.3 The Code applies to all companies involved with the A2P SMS service including the following companies/businesses:

- Mobile Network Operators (MNO)
- A2P SMS Aggregators or Aggregators
- Telecommunications Technology Providers (e.g., SCCP Providers)
- Cloud Communications Providers
- Brands and enterprises and any company engaging with their customers, via SMS

4.4 The Code does not address specifics of local laws or regulations; rather it shall be interpreted and applied in order to conform with the applicable legislation. Companies of the types referred in 4.3 from any country, can be signatories of the Code.

4.5 The Code also affects:

- consumers who opt-in to receive SMS messages via a service, or receive any kind of communication via SMS from a business they have a relationship with (e.g. text alerts, PIN codes, etc.)
- regulators and law enforcement bodies in charge of supervising the A2P SMS industry

5 Code Compliance

5.1 Once a company signs the Code they are known as Code Signatories, and as such the company agrees to abide by the Code at all times.

5.2 Code Signatories shall not engage in business with companies which knowingly breach the Code or applicable local laws.

5.3 The obligations of this Code must be adhered to promptly and effectively, taking all reasonable actions to ensure compliance to the code.

5.4 It is acknowledged that a Code Signatory may act in multiple roles across the A2P SMS value chain and it is the responsibility of the Company to ensure compliance with all relevant provisions.

5.5 Code Signatories must ensure that all relevant employees and associated parties are made aware of the Code.

6 Changes to the Code

6.1 MEF reserves the right to change to the Code from time to time, as a result of the ongoing outputs of the Future of Messaging Programme. The amended Code of Conduct remains binding.

6.2 MEF will notify all signatories of any changes to the Code and make each new version of the Code available on the Future of Messaging Programme website.

6.3 Furthermore, MEF reserves the right to amend the Code without any consultation with Code signatories if directed to do so by a court of law.

7 Requests to revoke the status of Code signatory

7.1 Companies may request MEF to revoke their status of Code Signatory at any time, either by post or e-mail.

7.2 MEF can take up to 30 (thirty) days to remove references to the company and/or revoke any Programme related rights obtained.

7.3 There will be no refund of any fees paid to MEF, regarding the Programme either for Programme participation or TEM badge signatory fees.

7.4 Companies have up to 30 (thirty) days to remove the Badge from their digital platforms and/or materials where it is being used.

8 Disclaimers

8.1 MEF's employees and its suppliers shall not be held liable for any consequences that may arise from either the implementation of the Code nor for the failure to implement the Code.

8.2 The Code does not constitute legal advice, nor is it warranted as legal advice.

9 Main Roles in the Code and Definitions

9.1 Consumer – this is the individual that is the destination of the A2P SMS message, the recipient of the SMS generated or the individual that sends a message to a Business via a Long Number or Short Code.

9.2 Enterprise or Brand – this is the company that wants to engage with the Consumer via SMS, e.g., bank, airline, government department etc.

9.3 Message Generator – this is the company who is sending the message, or on whose behalf the message is being sent, e.g. an enterprise or brand. The Message Generator in many cases will be the Enterprise or Brand.

9.4 Message Processor – this is any company in the ecosystem involved in the processing, routing, or carrying the message en-route to its final destination.

9.5 Message Terminator – this is any company in the ecosystem that is responsible for delivering the message to the consumer handset. This is usually a Mobile Network Operator (MNO).

9.6 Message Recipient – this is typically a person who is a customer or employee of the Enterprise or Brand. The Message Recipient is synonymous with the Consumer.

9.7 For Mobile Originated (MO) messages where the message is sent from a customer or employee to a business, then the Message Generator and Message Recipient roles above are reversed. For ease of reading, this document assumes

that all messages are Mobile Terminated (MT) and therefore the definitions above will apply.

10 The Code Principles

10.1 Code signatories shall not create, carry or deliver unsolicited A2P SMS messages.

Code signatories involved in A2P SMS creation, routing and delivery of A2P SMS messages must recognise that SMS is a powerful channel for businesses to interact with their consumers, on the understanding that consumers have consciously and explicitly authorised that interaction.

10.1.1 Message Generators (and all owners of the relationship with the consumer) shall ensure that consumers are informed of their rights and have opportunities to exercise meaningful choice and control over the messages they wish to receive. Hence, Message Generators shall not create A2P SMS messages destined to consumers who have not explicitly opted-in to receiving them.

10.1.2 Mechanisms and specificities of the opt-in process generally differ from country to country and/or for different types of communication, but usually include receiving a MO on a long code or short code or receiving permission via some electronic or physical form. For this purpose, the message originator must observe the applicable law/regulation and shall keep evidence of the opt-in readily available to show on demand by an authorised authority or the Compliance Committee.

10.2 Code signatories must accept that consumers shall be able to revoke their consent to be contacted.

Key to securing and maintaining trust in the A2P SMS channel is to ensure that consumers are always in control of the means by which and when they can be reached by enterprises. Therefore, it is key to provide consumers with the means to opt-out of interactions and relationships which they have previously authorised.

10.2.1 All Code signatories, but particularly Message Generators shall clearly communicate how consumers can opt-out of receiving messages in future.

10.2.2 Although local regulations vary, Code signatories should include opt-out guidance within the opt-in process itself.

10.2.3 Once a consumer has opted-out of the receipt of further communications, interaction with them must cease as soon as technically possible.

10.2.4 All Message Processors and Message Terminators shall stay vigilant and ensure that, to the best of their knowledge and ability, the Message Generators honour all opt-out requests received from their consumers and ensure that these requests are processed and terminated in a timely and reliable manner.

10.3 Code signatories must respect the legal or consumers' preferences regarding time and frequency of A2P SMS interaction.

Communication via SMS generally interrupts the Message Recipient and, therefore, extreme care must be observed regarding the timing and frequency of interaction.

Sending large volumes of messages that are not relevant to a recipient or at inconvenient hours of the day reduces the value of the message delivered as well as the overall A2P SMS channel, even if consent has been given by a recipient for the content being sent. It is key to recognise that one of the primary benefits of SMS is both the perception in the eye of the recipient and the reality that it is a trusted, clean and time-critical communications channel.

10.3.1 Message Generators, primarily, must respect the applicable law and consumers' preferences, regarding the timing and frequency of the messages sent (particularly if they have been explicitly indicated).

10.3.2 When there is no applicable law, and consumer preferences are unknown, common sense and best judgement should be observed (e.g. all promotional messages should be sent during waking hours, 8 am to 8 pm of the Message Recipient time zone, during a business/office working week, avoiding public holidays, days of religious observance, etc.).

10.3.3 All Code signatories shall take reasonable technical care by undertaking sufficient testing to prevent flooding incidents.

10.4 Secure and handle adequately consumers' personal data, ensuring the best data privacy practices when collecting, processing, and transmitting it.

The A2P SMS channel exposes recipient's personal data, namely their mobile number (personally identifiable data) and some associated content, to all companies involved in the generation, processing and termination of the messages. Personal data breaches have a very negative impact on consumers' trust in the A2P SMS channel and, therefore, best efforts must be taken with regard to data protection and security to try and avoid any such incident.

10.4.1 Code signatories shall comply with best practices and all relevant regulations governing customer data privacy.

10.4.2 Code signatories shall ensure that consumers are provided with clear, prominent and timely information regarding the company's data privacy practices.

10.4.3 When applicable, Code signatories shall ensure that customers are informed of their rights and have opportunities to exercise meaningful choice and control over their personal information.

10.4.4 When applicable, Code signatories shall seek consumer consent for any changes that materially affect the privacy of their personal information.

10.4.5 Code signatories shall limit the personal information that is collected from customers and subsequently retained, used, or shared.

10.4.6 Code signatories shall deploy state-of-the-art technology, making sure consumers' personal data is stored and passed on securely. Noting the availability of alternative solutions, Code signatories shall use strong encryption an all stages of personal data handling.

10.5 Code signatories shall not modify messages content or their metadata unless legitimately required for message delivery.

It is vital for the sustainability and growth of the A2P SMS channel that the messages generated are kept secure along the entire channel and delivered as they were intended by the Message Generator.

10.5.1 Unless for technical or regulatory reasons, messages' payload or their metadata Code signatories shall be kept unaltered, particularly elements such as SenderID or Global Title (GT), which are particularly relevant for identifying the companies involved in generating, processing or terminating A2P SMS messages.

10.6 Code signatories should deploy effective, proportionate risk-based procedures and tools to avoid consumer and/or business fraud.

A key aspect of ensuring a secure and compliant A2P SMS channel is the requirement that every company in the value chain takes appropriate care of its own infrastructure. This ensures reliable service provision with sufficient network system and capacity, while also aiming to combat the challenges which arise through fraudulent incidents where non-existent, insufficient or inadequate fraud protection tools and procedures are deployed along the value chain. The whole industry loses when fraud or any other industry incident occurs, as trust in the service or the value chain erodes.

10.6.1 Code signatories must be knowledgeable of the applicable the established rules that govern A2P SMS services in the markets through which the message is knowingly being delivered, in particular in the country where it is being terminated (for example, the use of short codes can be a legal requirement or a contractual obligation imposed by the terminating MNO).

10.6.2 Code signatories involved in the creation/delivery and termination of A2P SMS messages shall deploy all necessary tools and resources to protect and monitor their technical infrastructure for abnormal message volumes, formats or patterns to minimise the risk of not knowingly providing non-compliant service in terms of applicable law and signed contracts.

10.6.3 Code signatories shall properly identify and authenticate system users, such as by implementing password protection mechanisms and changing passwords to online systems (e.g., preventing ex-employees from using the channel illegitimately.

10.6.4 Code signatories shall limit physical access to systems.

10.6.5 Code signatories shall screen, train and monitor internal staff.

10.6.6 Code signatories shall ensure the protection of their assets that are accessible by suppliers and third parties.

10.6.7 Code signatories shall limit access to all message data to a "need to know" basis, by which, unless explicitly authorised, required by law or the Compliance Committee, or for the strict purpose of protecting the consumer recipient of the message or the involved industry players, message processors shall not access to message content to gain competitive advantage, drive business decisions, analyse competition or crunch content data to gain unfair business intelligence.

10.6.8 Code signatories shall ensure correct and secure operations of information processing.

10.6.9 Code signatories shall develop processes to ensure that all transactions and user activities are logged with appropriate audit trails.

10.6.10 Code signatories shall regularly test security systems and processes.

10.6.11 Code signatories shall ensure continuity of information security.

10.6.12 Code signatories shall develop a process to identify, address, and monitor security incidents and security-related complaints.

10.6.13 MNOs signatories of the Code must protect their network using all reasonable efforts to block the following (including but not limited to):

- SIM farms leveraging consumer/M2M SIM cards
- Grey routes
- Other networks that are using faking or Global Title manipulation to knowingly subvert their firewalls.
- HLR lookups that are not being used for bona fide routing or the delivery of SMS messages. In particular, HLR lookups should not contain the full IMSI
- Attempts at using Roaming Intercept fraud to intercept communications.

10.6.14 MNOs signatories of the Code shall deploy processes to avoid, SIM Swap or Porting fraud by ensuring thorough identity checks of their customers are undertaken.

10.6.15 Messaging Processors involved in signalling services, in particular, signalling providers shall ensure that only registered MNOs obtain access to the SS7 network.

10.6.16 Messaging Processors involved in signalling services, in particular, signalling providers should undertake thorough checks to ensure that the Global Title and point code ownership is legitimate.

10.6.17 Messaging Processors involved in signalling services, in particular, signalling providers should perform random checks to ensure that providers do not modify Global Title configurations after services go live.

10.6.18 Message Processors shall develop and deploy capabilities to (including but not limited to) detect, report and block traffic, if needed, based on suspicious traffic patterns, such as unusual volumes or a suspicious traffic origin:

- whitelist/blacklist specific message headers
- blacklist URLs or specific keywords part of the message content

10.6.19 Message Processors shall develop and deploy capabilities to (including but not limited to) prevent, detect and block looping incidents whereby the same message is sent between the same processors over and over again. Code signatories should:

- should block the looped messages immediately on discovery
- not invoice these messages, and credit notes should be issued by each provider to remove the messages involved in the looping incident.

10.7 Code signatories shall not access or utilise another company's infrastructure for any purpose for which they don't have explicit authorisation.

Companies must not seek competitive advantage by abusing any other company's infrastructure, accessing or using it in any way for which they do not have explicit authorisation. Also referred to as hacking, abuse assumes many different and constantly changing forms, as the industry develops technically.

10.7.1 Code signatories shall not knowingly create, operate or exploit SIM farms where SIM farms are outlawed or forbidden by the MNO.

10.7.2 Code signatories shall not knowingly manipulate Global Titles by using technical manipulation to subvert an MNO firewall (usually an attempt to deliver messages at no cost to the Message Processor or Message Terminator).

10.7.3 Code signatories shall not knowingly subvert an MNO firewall in attempt to extract SRI data either on an SMS or voice query layer.

10.7.4 Unless explicitly authorised/requested by the infrastructure owner or for regulatory reasons, code signatories shall not knowingly manipulate/change the original SenderID of a message or populate a senderID with fake or rotated numeric SenderIDs.

10.7.5 Code signatories shall not knowingly conduct split signalling on the A2P SMS MT, namely for following requests:

- SRI_SM
- FSM paths whereby the SRI_SM is sent via one MNO entity and the FSM by a different one

10.7.6 Code signatories shall not knowingly manipulate the TON/NPI settings of an SMS in order to send Short codes via international SS7 connections

10.8 Never hide your identity or use someone else's.

In most interactions between parties in the A2P SMS value chain, some form of identification is required, such as through the use of credentials or as part of the message metadata.

10.8.1 Code signatories shall use only their own legitimate credentials or identifier(s), and that further, they do not omit, fake or use someone else's credentials.

10.8.2 Code signatories shall not knowingly manipulate Global Titles to pretend to be someone else

10.8.3 Code signatories shall not knowingly use a Short Code or Long Code that is not owned/licensed and operated by them, for termination of A2P SMS messages.

10.9 Code signatory shall actively promote and educate all industry parties to ensure that every service offered is safe, reliable and complies with all relevant operational and legal requirements.

10.9.1 Code signatories shall communicate clear, sufficient and timely information to empower Enterprises to make safe and informed decisions about the correct use of A2P SMS services, particularly on topics such as:

- permitted and prohibited content types

- out-of-hours periods for message delivery

10.10 Code signatories shall proactively assist regulators, law enforcement agencies and other parties of the ecosystem to limit the scope and recurrence of fraudulent incidents and identify fraudulent actors within the ecosystem.

Given the global and complex nature of the A2P SMS delivery chain, fraud assumes many different formats and impacts on different technical infrastructures, often in multiple countries. Therefore, quick and open dialogue amongst all industry parties is fundamental to:

- Limit the scope of fraudulent incidents by enabling the industry to stop them, once detected, as quickly as possible. Rendering fraud ineffective is likely the most powerful deterrent for potential fraudulent companies.
- Identify and remove fraudsters from the A2P SMS value chain.

10.10.1 Code signatories shall investigate and report on the legitimacy of message headers if required by a terminating MNO, law enforcement agency, the Compliance Committee or any other value chain party.

10.10.2 Code signatories shall provide the information required by regulators, law enforcement bodies or other parties, which may help to stop a fraud incident or identify a fraudulent actor in a timely manner. This may include, for example, providing evidence of consumers' authorised opt-in and opt-out consent.

10.10.3 Code signatories shall report any suspected fraudulent activities, particularly calling out evidence and enough tracing information of unlawful activities, specifically SIM farms and Global Title Faking, as quickly as possible. The procedure is described in 11.

11 Logging Fraud Incidents

11.1 In the context of the Code, a fraud incident is one where SMS messages appear in the A2P SMS delivery chain, as a result of unlawful behaviour or as a consequence of a breach of a commercial contract.

11.2 When informed by a third party or identified through their own detection that they may be carrying unsolicited or fraudulent messages on their network, Code Signatories shall follow the steps and meet the timescales set out below:

- Within 5 (five) hours of discovering messages which, if delivered to the Messaging Terminator, result in unlawful behaviour or breach of a commercial contract (this includes but is not limited to Phishing or Spoofed messages) the company sending the messages is notified and asked to cease the messages immediately.
- If the messages have not ceased within 8 (eight) hours of the first request, the account is suspended.
- Within the next 8 (hour) hours following the account being suspended, the incident shall be reported to target MNO's fraud department and any other affected party.

- Within 8 (eight) hours of discovering suspected unsolicited messages, a request for evidence of opt-in consent is made to the company sending the messages, giving them 2 (two) business days to respond.
- Failure by the company to provide sufficient evidence opt-in consent, or to cease the suspicious traffic will result in their account being suspended and the company being reported to MNO's fraud department and any other affected party.
- Within 8 (eight) hours of discovering suspected Artificial Inflation of Traffic (AIT), a request for evidence of the service by the company sending the messages will be issued, giving them 2 (two) business days to respond.
- Failure by the company to provide sufficient evidence that this is a legitimate service or to cease the suspicious traffic will result in their account being suspended and the company reporting to MNO's fraud department and any other affected party.

12 Complaints

12.1 A **"**complaint**"** is defined as a complaint against a Code signatory or a notification of a breach of a previous Compliance Committee adjudication.

12.2 The **"**Compliance Committee**"** consists of three (or more) independent experts in the field of information and communications technology appointed by MEF.

12.3 Complaints have no appeal. The Compliance Committee decisions are final.

12.4 Any complainant may lodge a complaint against any Code signatory who, in the view of the complainant, has acted contrary to the provisions of this Code.

12.5 A complainant must lodge a complaint directly and solely based on the incident and breach of the Code.

12.6 A complaint may be directed at more than one signatory.

12.7 A complaint must be made within six months of the date of alleged breach of the Code. MEF may, at its discretion, accept a complaint after this six-month window, if the complainant provides a compelling reason for the delay in lodging the complaint.

12.8 Any complaint must be lodged with MEF using the complaint procedure information published on the Programme website.

12.9 The Complainant must not disclose any information about the complaint or the contents thereof.

12.10 In order to be reviewed by the Compliance Committee, as a minimum the complaint must contain the following information:

- the Company name of the Code signatory against whom the complaint is being made, or if its identity is not clear some other identifying information;
- the names and contact details of the complainant;
- to the extent that the information is known or available, identification of the part or parts of the Code which has allegedly been breached; and

- a detailed description of the actions or inactions that resulted in the alleged breach.

12.11 Any complaint lodged that does not contain the above information may be referred back to the complainant by MEF with a request to provide the missing information.

12.12 Notwithstanding if the complainant has not identified any or all of the relevant clauses of the Code, MEF may assign the relevant clauses based on the content provided. The complaint and subsequent response and adjudication will be limited to those clauses identified by either the complainant or MEF at the start of the matter.

12.13 MEF will not consider a complaint if it:

- does not address a Code signatory
- falls outside the remit of the Code
- is prima facie without merit, or
- is without sufficient grounds, taking into account factors such as malicious intent or made in bad faith.

12.14 If a complainant requests anonymity, the complainant's identity may, in exceptional circumstances, be withheld from the signatory at the discretion of the Compliance Committee. If the committee decides not to grant such anonymity, the complainant will be given a choice as to whether they wish to proceed.

12.15 At any point in the complaints process, a complainant may request via MEF that a complaint is withdrawn and MEF must comply with this request. However, if there is prima facie evidence of a breach of the Code which may affect consumers, the Compliance Committee is entitled to pursue a new complaint against the relevant Code signatory and may use any evidence submitted by the original complainant as part of the new complaint.

12.16 If the Compliance Committee believes that a complainant has not provided sufficient evidence for the Compliance Committee to be able to make a decision, the Compliance Committee may request that additional supporting information is provided. Should the complainant fail to provide the requested information, the Compliance Committee may close the complaint without it proceeding to adjudication.

12.17 The Code signatory named in the complaint or identified by the Compliance Committee on the basis of any identifying information included in the complaint is considered to be the respondent to the complaint. The respondent will be notified that a complaint has been lodged and that the Code's formal complaint procedure is being followed. The Compliance Committee will provide the respondent with a copy of the complaint, and any additional information relevant to the complaint.

12.18 The respondent will be given ten (10) working days to respond to the complaint, and to provide the Compliance Committee with any information the respondent deems relevant to the complaint, including any mitigating factors that the respondent wishes the Compliance Committee to consider. If the respondent so requests, an extension to this time period may be given at the discretion of the Compliance Committee.

12.19 Where a complaint involves any interaction with a customer or business partner, when requested to do so, the respondent must provide copies of relevant interactions and associated materials.

12.20 Providing incorrect or fraudulent information in response to a complaint or in response to any other request to provide information is itself a breach of the Code.

12.21 If the respondent fails to respond within 10 (ten) working days, it will be assumed that the respondent does not wish to respond.

12.22 Once (and if) the respondent has provided a response to the complaint, this response may be shared with the complainant. The complainant will be given five (5) working days to provide a response to the respondent's submission. If the complainant so requests, an extension to this time period may be given at the discretion of the Compliance Committee.

12.23 Once (and if) the complainant provides a response to the respondent's submission, this response will be provided to the respondent. The respondent will be given five (5) working days to provide a further response to the complainant's submission. If the respondent so requests, an extension to this time period may be given at the discretion of the Compliance Committee.

12.24 MEF will facilitate the complaint to the Compliance Committee, together with all materials submitted by the parties to the complaint.

12.25 The Compliance Committee will review:

- the complaint;
- any responses the respondent(s) and complainant have made to the complaint; and
- referencing the version(s) of the Code applicable at the time of the alleged breach.

12.26 If, during the investigation of the complaint, the Compliance Committee identifies potential breaches of clauses of the Code which were not specified in the complaint, the Compliance Committee may not rule on those clauses but may refer those potential breaches back to MEF. MEF may then lodge a new complaint against the Code signatory relating to the identified clauses.

12.27 The Compliance Committee may only make a ruling against the Code signatory(ies) identified as the respondent(s) to the complaint. If, during the investigation of the complaint, the Compliance Committee identifies potential breaches of clauses of the Code by a Code signatory other than the respondent(s), MEF may decide to lodge a new complaint against that signatory.

12.28 On the basis of the evidence presented, the Compliance Committee will decide whether there has been a breach of the clauses of the Code identified in the complaint. Each case will be considered and decided on its own merits. When making adjudications, previous precedent should be taken into account.

12.29 If the Compliance Committee determines that there has been a breach of the Code, then the Compliance Committee must determine appropriate sanctions. The Compliance Committee must take into consideration:

- any previous successful complaints made against the respondent in the past three years;
- any previous successful complaints of a similar nature;
- the nature and severity of the breach;
- the losses suffered by consumers, the complainant or any other parties involved;
- any efforts made by the respondent to resolve the matter; and
- any other factors that the Compliance Committee considers material.

12.30 Once the Compliance Committee has determined whether there has been a breach of the Code, and any sanctions, the Compliance Committee will provide MEF with a written report detailing these findings including any sanctions. MEF will provide the respondent and the complainant with access to the Compliance Committee's report.

12.31 The respondent must provide MEF with written confirmation of compliance with any applicable sanctions within ten (10) working days of receiving the Compliance Committee's report.

12.32 MEF will maintain a record of any and all complaints resolved through the formal complaint procedure, for a minimum period of three years after the complaint is closed.

13 Sanctions

13.1 Sanctions that may be imposed on a Code signatory found to be in breach of the Code include one or more of the following:

13.1.1 Withdrawal of the TEM Badge and consequent status of Code signatory, without any refund of fees paid regarding the Code or Programme.

13.1.2 If applicable, remove the signatory status of Programme participant, without any refund of fees paid regarding the Code or Programme.

13.2 MEF may, at its own discretion, send the Compliance Committee's written report to involved regulators and law enforcement bodies.

14 Adherence to the Code

14.1 Companies become Code signatories, by following the procedures defined at the Programme's website, signing this document and paying the respective fees.

14.2 Upon receipt of the documentation and fees, MEF has up to ten (10) days to send the Badge for use in line with respective terms and conditions.

Glossary

A2P SMS (Application to Person)
Messages originated by computer or application and intended for delivery to the subscribers of MNOs. A2P SMS is typically used by enterprise to communicate and share information with their customers, for example, bank balance alerts, retail order or delivery confirmation, appointment reminders and offers. A2P is generally used to send messages one way but two-way communication is possible in some markets.

Access Hacking, Hacking
The act of gaining access to an app, device, platform or any other IT infrastructure by someone without the permission of the owner.

Aggregator
A company that provides connectivity between MNOs and messaging routers.

Artificial Inflation of Traffic (AIT)
The act of artificially generating messages which are sent by a rogue party to itself in order to generate profit.

CPaaS (Communications Platform as a Service) Providers
Companies providing their customers (e.g., developers) a cloud-based platform where they can add real-time communications features (voice, video, and messaging) in their own applications without needing to build backend infrastructure and interfaces.

Firewall
A filtering system which enables MNOs to monitor, detect, block and report suspicious or unauthorised messages destined for delivery through their network and to their subscribers

FSM (Forward Short Message)
The second of two SS7 requests sent by an SMSC when a message is being sent, the first being an SRI. Both an SRI and FSM request are required to send a message.

Global Title (GT)
An address used in the SCCP protocol for routing messages through an MNOs network. A Global Title is a unique address which refers to a single destination, though in practice, destinations can change over time.

Grey Route
A connection used for the delivery of enterprise messages, but which is not authorised for that use, for example, where the absence of a commercial agreement for a connection is exploited as a lower cost option at the expense of the terminating MNO.

HLR (Home Location Register)

The database within a GSM Network which stores all mobile subscriber data, including the subscriber's location (eg, home or roaming), phone status, (eg, on, off, inbox full etc) and their mobile network.

IMSI (International Mobile Subscriber Identity)
A unique number, usually fifteen digits, which identifies a GSM mobile network subscriber.

MAP Global Title Faking
Manipulation of specific technical parameters or disguising a message sender's true identity in order to gain access to an MNO's network to deliver messages which would otherwise be flagged as unauthorised and rejected by an MNO.

Message Generator
This is the company or brand from which the message is being sent. Even if the message is technically created by a 3rd party on behalf of the brand, the brand is still regarded as a message generator.

Message Processor
This is any company in the ecosystem that is involved in the processing, routing, or carrying the message en-route to its final destination.

Message Recipient
This is typically a person that is a customer or employee of the Message Generator.

Message Terminator
This is any company in the ecosystem that is responsible for delivering the message to the consumer handset. Usually a Mobile Network Operator.

Mobile Network Operator; Mobile Operator (MNO)
An MNO provides wireless or mobile communication services and owns or controls all of the elements of the network infrastructure necessary to deliver services to a mobile subscriber. All MNOs must also own or control access to a radio spectrum license which has been issued by a regulatory or government body. An MNO typically controls provisioning, billing and customer care, marketing and engineering organisations needed to sell, deliver and bill for services, though these systems and functions can be outsourced.

Mobile Originated (MO)
This describes the source of a sent message, ie, at the start of the end to end message delivery chain. See also Originating Mobile Operator.

MNP (Mobile Number Portability)
This lets a mobile subscriber move from one MNO to another while keeping their number. MNP has made it impossible to determine the mobile network of an MSISDN by its prefix.

MSISDN (Mobile Station International Subscriber Directory Number)
The unique mobile phone number attached to a SIM card used in a mobile device.

MSC (Mobile Switching Centre)
An MSC routes messages, performs service billing and interfaces with other telecoms networks, such as the public switched telephone network (PSTN). All forms of communication, whether between two mobile phones or between a mobile phone and a landline telephone, travel through the MSC.

Mobile Terminated (MT)
This describes the destination of a sent message, ie, at the end of the end to end message delivery chain. See also Terminating Mobile Operator.

NPI Settings
See TON/NPI Settings

Originating Mobile Operator; Originating MNO
The MNO at the start of the end to end message delivery chain which accepts messages from a messaging provider for onward delivery.

Originator/SenderID
The term used to describe the number or word which identifies who a message is from upon receipt. It is also known as a SenderID. An alphanumeric originator enables a brand name to be set as the identified 'sender' of a message.

Phishing, SMS Phishing, SMiShing
The act of misleading a mobile subscriber by presenting to be a known and trusted party to gain access to online systems, accounts or data such as credit card, banking information or passwords for malicious reasons.
Roaming Intercept Fraud/SMS Roaming Intercept Fraud
The act of deliberately intercepting a message while a consumer is roaming.

SCCP Provider
A company which manages the SCCP layer protocol.

SCCP Global Title Faking
The act of sending a message in a way that deceives the terminating MNO about the true identity of the sender through the misuse of a Global Title.

Short Code, Short Number
A special numbers, significantly shorter than a full 11-digit phone number, which can be used to send SMS and MMS messages.

Signalling Providers
Companies providing the connectivity that enables roaming and messaging between an MNO and its roaming partners. It ensures continuity of service for mobile users by

enabling them to make or receive mobile calls, send or receive SMS and use mobile internet while travelling all around the globe.

SIM; SIM Card (Subscriber Identity Module)
A smart card inserted into a mobile device which carries a unique identification number, stores personal data and prevents operation of the device if removed.

SIM Farms
A method of using a bank of SIM cards for the delivery of messages for which the SIMs are not designated, for example retail SIMs intended for use by individual mobile subscribers which are instead used for the delivery of enterprise messages.

SIM Swap Fraud or Porting Fraud
The act of obtaining control of a mobile number by cancelling the SIM linked to a consumer's handset and activating a new SIM linked to a different handset, and so causing all calls and texts to be routed to and from a different handset, outside of the control of the consumer.

SMS (Short Message Services)
A text messaging service component of phone, web, or mobile communication systems which uses standardised communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

SMSC (Short Message Service Centre)
An element within an MNO's network which receives messages from mobile network users (enterprise and individual mobile subscribers), stores, forwards and delivers messages to mobile network users, as well as maintaining unique timestamps in messages.

Split signalling
In the context of the Code, it refers to the use of different Global Titles for operations which require distinct calls to an external infrastructure, e.g., SRI and FSM calls are required to send a message.

SRI (Send Routing Information)
This is the first of two SS7 requests sent by a SMSC when a message is being sent, the second of which is an FSM request. An SRI request is made by the originating MNO's SMSC to the HLR/VLR to request routing information and determine the IMSI of a mobile subscriber. Both an SRI and FSM request are required to send a message.

SRI_SM
It is the MAP-Send-Routing-Info-For-SM query message. It is normally issued by the SMSC to the HLR, since the SMSC does not know the location of the terminating subscriber.

STP (Signal Transfer Point)

A router that relays SS7 Network messages between signalling end and signalling transfer points. STPs are typically provisioned in mated pairs to meet stringent reliability requirements.

Spam
A broad term for an unsolicited message, namely, one which is not wanted by the recipient, whether the message has been sent with good intentions or maliciously.

SMS Originator Spoofing, Spoofing
The act of changing a message originator to someone or something known to the recipient to hide the sender's true identity.

SS7 (Signalling System 7)
A set of telephony signalling protocols that enable the sending of SMS messages as well as performing number translation, local number portability, prepaid billing and other mass market services. SS7 is not permitted in some regions.

Terminating Mobile Network Operator; Terminating MNO
The MNO at the end of the end to end message delivery chain to which your customers are subscribed.

Traffic
A common term used to refer to the movement of messages, eg, "the [SMS] traffic has been successfully delivered."

TON (Type Of Number)/NPI (Numbering Plan Identification) Settings
Both are fields of an "Address", in GSM 03.40 standard messages. They allow senders to manage originator and destination settings.

VLR (Visitor Location Register)
A database which contains information about mobile subscribers roaming within an MSC's location area. Its primary role is to minimise the number of queries that MSCs have to make to the HLR.