



Code of Practice

Mobile Spam

0.9

26 January 2006

This is a non-binding permanent reference document of the GSM Association.

Security Classification Category (see next page)

<i>This is an UNRESTRICTED document.</i>
--

Security Classification - Unrestricted

This document is subject to copyright protection.

The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association.

Copyright Notice

Copyright © 2006 GSM Association

GSM™ and the GSM Logo™ are registered and the property of the GSM Association.

Table of Contents

1	Executive Summary	4
2	The Code of Practice.....	5
3	Implementation and Review	7

1 Executive Summary

1.1 About this document

The Mobile Spam Code of Practice ('the Code') is a voluntary non-legally binding document reflecting a commitment by operators and the GSMA to act against mobile spam and minimise the impact it has on customers.

Some of the principles and commitments within the Code are already contained in the laws of various countries. However, against a background of disparity in national legal environments, the mobile industry has identified the need to work together to adopt consistent approaches to dealing with spam and share best practice.

1.1.1 Scope

The Code applies to unsolicited communications sent via SMS and MMS and includes: commercial messages sent to customers without consent, commercial messages sent to customers encouraging them directly or indirectly to call or send a message to a premium rate number, and bulk fraudulent messages sent to customers (e.g. faking, spoofing or scam messages).

1.1.2 Purpose

Under the Code, the mobile operators that are signatories commit to:

- Include anti-spam conditions in all new contracts with third party suppliers
- Provide a mechanism that ensures appropriate customer consent and effective customer control with respect to mobile operators' own marketing communications
- Work co-operatively with other mobile operators to address spam issues
- Provide customers with information and resources to help them minimise the levels and impact of mobile spam
- Undertake other anti-spam activities to minimise the level and impact of mobile spam
- Encourage governments and regulators to support industry.

The signatories will work in good faith to implement the commitments highlighted above and the GSMA will monitor the adoption and implementation of the Code. The GSMA and signatories to this Code of Practice will continue to examine issues associated with other types of spam and unsolicited communications and will update the Code as appropriate.

2 THE CODE OF PRACTICE

This Code of Practice demonstrates mobile operators' commitment to fight proactively mobile spam and minimise the impact that it has on customers.

This Code of Practice applies to unsolicited communications sent via SMS and MMS (referred to as 'mobile spam') and specifically includes¹:

- i) Commercial short messages or multimedia messages sent to customers without consent as required by national law (e.g. marketing messages).
- ii) Commercial short messages or multimedia messages sent to customers encouraging them directly or indirectly to call or send a short message or other electronic communication to a premium rate number.
- iii) Short messages or multimedia messages sent to customers in bulk and which are fraudulent (e.g. faking, spoofing or scam messages).

For the purpose of this Code of Practice, "commercial short messages or multimedia messages"² means SMS or MMS messages designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial activity or exercising a regulated profession.

The mobile operators that are signatories to this Code of Practice commit to:

1. Include anti-spam conditions in all new contracts with third party suppliers. In these third party supplier contracts, conditions should include:
 - A commitment to not send or initiate mobile spam.
 - A commitment to respect the consent requirements set by relevant national legislation or self-regulatory mechanisms in force.
 - A commitment to provide customers with obvious, clear and efficient means to opt-out of receiving further SMS or MMS marketing communications.
 - Potential penalties for breaching the anti-spam commitments, including possible suspension and/or termination of contracts.
2. Provide a mechanism that ensures effective customer control with respect to mobile operators' own marketing communications via SMS or MMS, in-line with consent requirements set out in national legislation.

The means of enabling consent could include providing customers with prior 'opt-in' consent mechanisms (where customers opt-in to receive communications) and/or 'opt-out' mechanisms (where customers are given the opportunity to opt-out of any future communications).

Operators also commit to:

- Ensure that the processes they use to obtain consent are clear and transparent and that records are kept of the type of consent obtained from customers, including how and when consent was received.

¹ The following terms reflect standard terminology used by the GSMA in official and general documents including the AA.19 and AA.40 Addendums to the International GSM Roaming Agreement: SMS & MMS Interworking Agreements and include WAP Push messages. Faking and spoofing are described in detail in the GSMA's official document IR.70 SMS SS7 Fraud.

² As distinguished from service related messages provided by mobile operators. For example, messages relating to roaming, voicemail or customer services.

- Provide customers with obvious, clear and efficient means to opt-out of receiving further operator mobile marketing communications sent via SMS or MMS.
3. Work co-operatively with other mobile operators to investigate cases of mobile spam transmitted across networks and take action where appropriate.
 4. Provide customers with information and resources to help them minimise the level and impact of mobile spam. These should include:
 - Provision of information on operators' anti-spam policies, relevant legislation and local codes of practice.
 - Advice on how to handle incidents of suspected spam, through their customer services contacts, in print and/or on their websites.
 - Provision of mobile spam reporting facilities. For example, through their customer services contacts, website and/or via a 'shortcode' for customers to forward suspected mobile spam to.
 5. Undertake activities designed to minimise the level and impact of mobile spam, including:
 - Ensure that they have an anti-spam policy that prohibits the use of the mobile network for initiating or sending mobile spam.
 - Review customer contracts, Terms & Conditions and/or Acceptable Use Policies, to ensure that up-to-date and relevant anti-spam conditions are included. For example, conditions indicating that complaints may be investigated (including co-operation with relevant public authorities as appropriate) and that the operator may terminate its service to a customer who originates mobile spam.
 - Prioritise and investigate customer complaints regarding mobile spam, as appropriate, take action and report cases to the relevant public authorities, where appropriate.
 - Monitor networks for signs of mobile spam and take proactive action to eliminate mobile spam, subject to the requirements of national legislation.
 - Share information on best practice and co-operate with other mobile operators, nationally and internationally, to minimise mobile spam sent across networks. This should include considering the adoption of GSMA recommended techniques for detecting and dealing with the international transmission of fraudulent mobile spam and/or unsolicited SMS and MMS, which encourage a premium rate response and taking measures to ensure that the operators originating SMS and MMS are correctly identified i.e. to prevent "spoofing" of the sender's identification.
 6. Encourage governments and regulators to:
 - Support industry self-regulatory mechanisms.
 - Support the development of responsible mobile marketing and premium rate industries. For example, through support for codes of practice that promote effective consent principles, transparency and clear pricing.
 - Support investigation of spam abuses and fraud. For example, by addressing any data protection / privacy law issues or premium rate payment issues that may hamper mobile operators' ability to investigate mobile spam abuses.
 - Support mobile operators in their efforts to combat mobile spam at the network level. For example, by permitting the use of network level filtering to identify and prevent mobile spam reaching customers.
 - Create/support an environment that penalises those that send unsolicited SMS or MMS messages that encourage a premium rate response. For example, allow mobile operators to

withhold payments to suspected mobile spam destinations, pending investigation of their spam activities by the relevant public authorities.

3 IMPLEMENTATION AND REVIEW

The signatories to this Code of Practice will work in good faith to implement the commitments and measures listed above. Implementation timescales may vary for the different commitments and measures, depending on their technical complexity and the duration of existing contracts. The Code of Practice constitutes the intention of the GSMA and signatories to implement the measures as soon as practical in order to serve their customers interests.

The GSMA commits to:

- Monitor the adoption and implementation of the Code of Practice and the need for any further action.
- Invite signatories periodically to provide more detailed information on the effectiveness and proportionality of the measures taken.
- Assist operators in resolving inter-network mobile spam issues and in dealing with cases of persistent illegal or fraudulent activity, related to mobile spam.