INTERNET INDUSTRY
SPAM CODE OF PRACTICE

A Code for Internet and Email Service Providers

CO-REGULATION IN MATTERS RELATING TO SPAM EMAIL

(CONSISTENT WITH THE REQUIREMENTS OF THE SPAM ACT 2003 AND TELECOMMUNICATIONS ACT 1997 TO THE EXTENT IT RELATES TO THE SPAM ACT)

DECEMBER 2005
Version 1.0

Internet Industry Association
www.iia.net.au

EXPLANATORY STATEMENT

This is the Explanatory Statement for the IIA Spam Code of Practice (the Code). This Explanatory Statement outlines the purpose of the Code and the factors that have been taken into account in its development.

Background

This Code seeks to establish industry wide practices and procedures relating to those Electronic Messages (as that term is defined by the *Spam Act 2003* ("the Act")) that are Spam email.

There are enormous benefits brought by email to Australian businesses and End Users as a low cost and rapid communications medium. Access to email remains a primary reason for many Australians going online.

The phenomenon of Spam has and continues to materially impact on email as a communications medium. Spam currently is considered to constitute over half the volume of email globally and imposes costs and inconvenience on End Users and Service Providers alike. Further Spam may, in addition to being in contravention of the Act, also contain illegal content, be offensive or contain malicious codes and viruses.

In order to respond to the issues created by Spam a diverse strategy must be employed consisting of five complementary elements:

- strong, effective domestic legislation;
- education of end users;
- action by the e-marketing and ISP industries;
- technological solutions; and
- international cooperative efforts.

In furthering these elements, industry including the IIA, WAIA, SAIA and like organisations have been active in devising initiatives designed to combat the Spam problem by providing information to End Users, reviewing operational procedures and implementing "nospam" policies.

This Code has been drafted with a view to ensuring it does not unduly impede legitimate business activities conducted over the Internet while also recognising that action must be taken by Service Providers to assist with the minimisation of Spam, and the detriment caused by Spam. Further, the code has been drafted with regard to the Australian e-Marketing Code of Practice and the SMS Issues Code which both deal with Spam related issues.

Lastly regard has been given to relevant RFCs (Requests for Comment) and to the RFC process in general. RFCs are the working notes of the Internet research and development community. These documents contain protocol and model descriptions, experimental results, and reviews. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs. New standards may be proposed and published on line, as a RFC. The Internet Engineering Task Force is a consensus-building body that facilitates discussion, and eventually a new standard may be established, but the reference number/name for the standard retains the acronym RFC, e.g. the official standard for email is RFC 822. The Taskforce is mindful of this being the appropriate medium for the development of new Internet standards.

Section 112 of the *Telecommunications Act 1997* ("the Telecommunications Act") sets out the intention of the Commonwealth Parliament that bodies and associations in the telecommunications industry develop industry codes relating to the telecommunications activities of those bodies. Subsection 113(3) of the Telecommunications Act sets out examples of topics that could be included in a code and includes:

(a) procedures to be followed by Service Providers in dealing with Spam (including procedures relating to the provision or use of regularly updated software for filtering Spam);

(b) giving Subscribers information about the availability, use and appropriate application of software for filtering Spam;

(c) action to be taken to assist in the development and evaluation of software for filtering Spam;

(d) action to be taken in order to minimise or prevent the sending or delivery of Spam, including the:

    (i) configuration of servers so as to minimise or prevent the sending or delivery of Spam; and

    (ii) shutdown of open relay servers.

The Australian Communications and Media Authority (ACMA) is responsible for administering a range of technical and consumer issues relating to telecommunications and is encouraging industry to develop voluntary codes of practice and technical standards where they are in the public interest and do not impose undue financial and administrative burdens on industry participants. Industry codes may be registered by the ACMA, which then enables the ACMA to require an industry participant to comply with a code.

Code Development and Review

The IIA Spam Taskforce ("Taskforce") developing the Code has representation from a large cross section of Service Providers and other interested parties. The development process for the Code is as follows:

(a) an initial draft code is produced which in the view of the Taskforce achieves the objectives and will be acceptable to industry ("the Preliminary Draft"). The Taskforce will have regard to relevant ACMA guidelines in terms of the Code development and the Telecommunications Act in respect of matters to be addressed in the Code

(b) The Taskforce will provide regulatory bodies including ACMA, the ACCC, the TIO, and consumer bodies such as the Australia Consumers Association, ISOC-AU and CAUBE with the Preliminary Draft for consideration and comment.

(c) The Taskforce will consider and incorporate the recommendations from the reviewers of the Preliminary Draft as appropriate. The Taskforce will provide reasons as to why any suggestions or comments have not been incorporated.

(d) The revised document (the Code) will then be released for the statutory public consultation period.

(e) Further consultation will be undertaken by the Taskforce as required and all comments will be considered. The Taskforce will document which recommendations have been incorporated and in respect of those (if any), which it is not able to incorporate, it will provide the reasons why they could not be accommodated. This record will form part of the taskforce's documentary submission to the ACMA when applying for registration of the code.

Current Regulatory Arrangements

The Spam Act 2003 ("the Act") came into effect on 10 April 2004. Under the new law it is illegal to send, or cause to be sent, 'unsolicited commercial electronic messages' that have an Australian link. A message has an 'Australian link' if it either originates or was commissioned in Australia, or originates overseas but has been sent to an address accessed in Australia.

The Act covers electronic messages – emails, mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (IM) – of a commercial nature. However, the Act does not cover voice or fax telemarketing. The Act sets out penalties of up to $1.1 million a day for repeat corporate offenders. The Act also outlaws the use of address harvesting software or lists produced with such software.

The Telecommunications Act also specifically lists certain matters relating to the handling of Spam as an example of the priority areas for the development of industry codes, but does not otherwise impose any specific requirements on the industry.

The Act addresses the Spam problem principally by targeting senders of Spam. However since senders of Spam require the services of Service Providers in order to send their Spam, enlisting the support of those Service Providers has the potential of being an efficient and also a more pro-active way of addressing the Spam problem. This illustrates the scope for the introduction of a co-regulatory code on Spam for the Internet industry.

How the Code Builds on and Enhances the Current Regulatory Arrangements

The Code establishes minimum acceptable practices for Service Providers to follow in relation to:

(a) providing useful information to End Users on how to minimise Spam;

(b) dealing with Reports from End Users and Complaints from Subscribers regarding Spam;

(c) interacting with Law Enforcement Agencies (LEA) on Spam related matters within the context of the requirement to maintain the confidentiality of an End User's personal information and when such personal information may be lawfully disclosed; and

(d) technical initiatives.

This is considered to be essential to the process of reducing Spam in Australia.

How the Objectives will be Achieved

This Code will apply to carriage service providers and email service providers insofar as they fall within the relevant definitions under the Telecommunications Act and are involved in the generation, transmission or delivery of Spam. Industry compliance with the Code is encouraged through registration with the ACMA.

Anticipated Benefits to Consumers

Registration of this Code with the ACMA will benefit consumers by establishing practices that will assist in the minimisation of Spam in Australia and also by providing information to End Users about both preventative and curative steps that may be taken in respect of Spam. The rules and principles have been written in plain English to ensure they are easily understood and consistently applied throughout the industry by Service Providers.

Anticipated Benefits to Industry

Service Providers will benefit from the registration of this Code with the ACMA through the expectation that the existence and observance of the rules and guidelines within the Code will assist with the minimisation of Spam in Australia and hence the generation of higher levels of Subscriber satisfaction and improved operational efficiency.

The Code rules, examples and explanatory comments have been framed in an easily understood manner providing a degree of certainty of understanding leading to consistency in their application throughout the industry by Service Providers.

Anticipated Cost to industry

It is expected that Service Providers will incur initial and ongoing costs in relation to compliance with this Code, depending on each Service Provider's current practices. Service Providers are expected to incur initial and ongoing costs in relation to the education and training of staff, development or enhancement of policies and procedures, development or modification of internal systems and employment of additional staff. Service Providers that are subject to the Privacy Act are also expected to incur costs in reviewing their current privacy management practices as certain of the obligations imposed by this Code will require such a review to ensure compliance with the Privacy Act.

CONTENTS

EXPLANATORY STATEMENT 2

CONTENTS 7

PART A – PRELIMINARY 8

1. INTRODUCTION AND REGISTRATION WITH THE ACMA 8

2. SCOPE AND OBJECTIVES 9

3. TERMINOLOGY AND INTERPRETATION 10

CODE RULES 15

PART B – PROVISION OF INFORMATION 15

4. PROVISION OF INFORMATION 15

PART C – LAW ENFORCEMENT ISSUES 17

5. LAW ENFORCEMENT COOPERATION 17

PART D – SPAM FILTERS 18

6. MAKING SPAM FILTERS AVAILABLE 18

PART E – SERVICE PROVIDER OBLIGATIONS 19

7. OPEN RELAYS AND OPEN PROXIES 19

8. IP ADDRESS INFORMATION 19

9. BEST PRACTICES 191

PART F – REPORTING SPAM 21

10. GENERAL REQUIREMENTS 21

PART G – COMPLAINT HANDLING 23

11. COMPLAINTS FROM SUBSCRIBERS ABOUT SPAM 23

12. COMPLAINTS REGARDING BREACH OF THE CODE BY SERVICE PROVIDERS 26

PART H - MISCELLANEOUS 26

13. DATE OF IMPLEMENTATION 26

14. DATES OF REVIEW 26

SCHEDULE 1 – LIST OF CONTRIBUTORS 27

PART A – PRELIMINARY

1. Introduction and Registration with the ACMA

1.1 Introduction

1.1.1 As stated in subsection 112(3) of the Telecommunications Act Parliament intends that public interest considerations within codes are addressed in a way that does not impose undue financial and administrative burdens on participants in the section of the telecommunications industry that the Code affects, in this case Service Providers. Matters to which the ACMA must have regard include:

(a) the number of End Users who would likely benefit from a code

(b) the extent to which those End Users are residential or small business in nature;

(c) the legitimate business interests of Service Providers; and

(d) the public interest.

1.1.2 Section 113 of the Telecommunications Act sets out examples of matters that may be dealt with by industry codes and specifically includes a reference to matters relating to Spam.

1.1.3 To give effect to Parliament's intent as expressed in subsection 112(3) and section 113 of the Telecommunications Act, this Code addresses the handling of certain Spam related matters by Service Providers and has been facilitated by the IIA through the Taskforce. Through participation on the Taskforce by, amongst other parties, industry representative bodies such as the IIA, WAIA and SAIA the Taskforce is representative of the Australian Internet Industry. Importantly the Code development process has also involved input from other industry and non-industry stakeholders including Government regulators, agencies and consumer organisations. **Schedule 1** lists those industry and non industry players who have contributed to the development of this Code.

1.1.4 If there is a conflict between the requirements of this Code and any requirements imposed on Service Providers by statute, the Service Provider will not be in breach of this Code by complying with the requirements of the statute.

1.1.5 For the purposes of this Code, the acronyms, definitions and interpretations set out in clause 3 apply unless otherwise stated.

1.2 Registration with the ACMA

This Code is to be submitted to the ACMA for registration pursuant to section 117 of the Telecommunications Act.

2. Scope and Objectives

2.1 Scope

2.1.1 This Code applies to the following sections of the telecommunications industry under section 110 of the Telecommunications Act:

(a) Carriage Service Providers; and

(b) Electronic messaging service providers.

2.1.2 This Code sets out rules and guidelines regarding Spam issues that arise in relation to Telecommunications Activities as defined in Section 109 of the Telecommunications Act. Telecommunications Activities are defined as:

(a) carrying on business as a carriage service provider; or

(b) supplying goods or services for use in connection with the supply of a listed carriage service; or

(c) carrying on business as an electronic messaging service provider

This Code only applies to Electronic Messages in so far as they are email.

2.1.3 The requirements of this Code apply to Service Providers irrespective of the size of the organisation.

2.1.4 This Code excludes:

(a) matters relating to e-marketing activities which are addressed in the Australian e-Marketing code of Practice and

(b) matters relating to the use SMS for the delivery of marketing messages to mobile telephone customers addressed by the SMS Issues Code.

2.2 Objectives

2.2.1 The objectives of this Code are to:

(a) provide rules and guidelines for Service Providers to ensure compliance with their legal obligations and promote the adoption of responsible processes and procedures for dealing with Spam;

(b) ensure these rules and guidelines are developed in such a way as to achieve a balance between legitimate industry interests and viability and End User interests;

(c) reduce the volume of Spam being created within the Australian internet;

(d) reduce the volume of Spam being delivered to Australian email boxes;

(e) promote End User confidence in and encourage the use of the Internet; and

(f) provide a transparent mechanism for complaint handling by Service Providers in relation to Spam and any breaches of this Code, and ensuring that complaints are handled in a fair and efficient manner.

2.2.2 In seeking to achieve its objectives this Code applies the following principles:

(a) ensure there is a balance between legitimate industry interests and viability and End User interests;

(b) any rules should not adversely affect the commercial viability of Service Providers and the services they make available; and

(c) that Spam is an inherent risk when using the Internet and as such Service Providers and End Users each have responsibilities in attempting to minimise the Spam burden.

3. Terminology and Interpretation

3.1 Definitions

Acceptable Use Policy	means the policy of a Service Provider governing the appropriate use amongst other things of email and the Service Provider's network and services, or any terms and conditions upon which a Service Provider provides an email service, including where appropriate the grounds on which a Subscriber's service can be terminated by the Service Provider.

account	has the meaning given in Section 4 of the Act.
Act	means the *Spam Act, 2003* (Cth).
Code	means this Code of Practice.
Complaint	means an expression of dissatisfaction or grievance made to a Service Provider by a Subscriber, but does not include a Report.
Content	means all forms of information and, without limitation, includes text, pictures, animation, video and sound recording, separately or combined and may include Software.
Electronic Message	has the meaning given in subsection 5(1) of the Act.
Email Service Provider (or ESP)	means an electronic messaging service provider, including a provider of web-based e-mail services, within the meaning of section 108A of the Telecommunications Act, which provider may or may not also be an ISP.
End User	means any person with access to an email account.
Home Page	means in relation to a Service Provider, those Web Pages or interactive services used by the Service Provider to communicate to Subscribers and End Users including to provide information regarding products or services of the Service Provider.
IIA Board	means the Board of Directors of the IIA.
International ESP	means an ESP which has its central management and control located outside Australia and which provides an Email service which: (a) hosts the contents of emails received or sent by an End User on computers located outside Australia;

	(b) has some End Users located in Australia; and (c) has a greater number of End-Users located outside Australia than in Australia.
Internet	means the public network of computer networks known by that name.
Internet Address	means the electronic address of Content housed on the Internet.
Internet Service Provider (or ISP)	has the same meaning as in Schedule 5 to the *Broadcasting Services Act,* 1992 (as amended) to the extent that they are providers of email services.
person	includes partnerships, bodies corporate and the Crown.
Privacy Act	means the *Privacy Act, 1988* (Cth).
Report	means a notification to a Service Provider that Spam appears to have been sent through the Service Provider's network, or that there appears to have been a breach of the Service Provider's Acceptable Use Policy by a Subscriber of the Service Provider that is related to Spam.
Service Providers	refers collectively to ISPs, ESPs, and International ESPs.
Spam	means commercial electronic messages that: (a) are unsolicited within the meaning of section 16 of the Act; or (b) do not include accurate sender information as required by section 17 of the Act; or (c) do not contain a functional unsubscribe facility as required by section 18 of the Act.'
Spam Filter	means any product (including software), device solution or service that is designed to minimise, eliminate or quarantine suspected Spam.

Subscriber	means an End User with a contractual relationship with a Service Provider.
Taskforce	means the Spam Taskforce as constituted from time to time by the IIA. The current membership of the Taskforce is set out in Schedule 1.
Telecommunications Act	means the *Telecommunications Act, 1997* (Cth).
Trade Practices Act	means the *Trade Practices Act, 1974* (Cth).
Web Page	means a file of Content accessible on the World Wide Web by requesting a single Internet Address.

3.2 Interpretation

In this Code, unless the contrary appears:

(a) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(b) words in the singular include the plural and vice versa;

(c) words importing persons include a body whether corporate, politic or otherwise;

(d) a reference to a person includes a reference to the person's executors, administrators, successors, officers, employees, volunteers, agents and/or subcontractors (including but not limited to, persons taking by novation) and assigns; and

(e) where documents are referred to in this Code by means of Internet Addresses, the Internet Addresses are intended for reference only and the operation of the Code will not be affected where the document referred to is subsequently relocated to another Internet Address.

3.3 Abbreviations

ACMA: Australian Communications and Media Authority

ACCC:	Australian Competition and Consumer Commission
ACIF:	Australian Communications Industry Forum
AUP:	Acceptable Use Policy
CAUBE:	Coalition Against Unsolicited Bulk Email
ESP:	Email Service Provider
IIA	Internet Industry Association
ISOC-AU	Internet Society of Australia
ISP:	Internet Service Provider
RFC	Request For Comments
SAIA:	South Australian Internet Association
SMS/MMS:	Short Message Service/Multimedia Message Service
TIO:	Telecommunications Industry Ombudsman
WAIA:	Western Australian Internet Association

CODE RULES

PART B – PROVISION OF INFORMATION

4. Provision of Information

4.1 Subject to Clause 4.4, Service Providers must take reasonable steps to:

(a) inform Subscribers that they must comply with the Act and otherwise not engage in the practices which would result in a breach of the Act;

(b) inform Subscribers of the existence of any Code of Practice registered with the ACMA applicable to Spam;

(c) inform Subscribers of any relevant changes or additions to legislation applicable to Spam;

(d) warn Subscribers of the consequences of breaching a Service Provider's Acceptable Use Policy in relation to the sending of Spam, including where applicable, the potential for termination/suspension of the Subscriber's account;

(e) advise Subscribers of:

(i) methods of minimising the receipt of Spam;

(ii) the availability of Spam Filters;

(iii) their right to make complaints to the ACMA about Spam and procedures by which such complaints can be made;

(iv) their right to make complaints to other bodies about Spam where the content is in some other way offensive or contrary to law. For example to the ACMA about Spam that contains material that promotes or advertises content that is likely to cause offence to a reasonable adult, to the Privacy Commissioner if for example the Spam appears to be the result of misuse of personal information and to the ACCC about Spam that contains misleading and deceptive material or material that is likely to mislead or deceive or otherwise contravenes the Trade Practices Act;

(f) inform Subscribers whether Electronic Messages addressed to them are subjected by the Service Provider to a Spam Filter by default, and provide a non-technical overview of the operations of that Spam Filter; and

(g) warn subscribers that the use of a Spam Filter may result in the loss of some legitimate Electronic Messages.

4.2 In respect of the preceding subparagraphs (a)-(e), 'reasonable steps' must include:

(a) the provision of information in an Acceptable Use Policy;

(b) providing a link from a reasonably prominent position on the Service Provider's Home Page to an information resource created for that purpose;

(c) providing a link from a reasonably prominent position on the Service Provider's Home Page to this Code;

(d) a statement to the effect that the AUP defines Spam at a minimum by the indicia set out in the Act;

(e) a statement to the effect that there are suspension and terminations provisions in the AUP which may be enforced at the Service Provider's discretion.

4.3 In respect of 4.1 (a) – (e), 'reasonable steps' may also include providing a link to the ACMA web site on Spam.

4.4 The obligations set out in paragraphs 4.1(a), 4.1(b), 4.1(c) and 4.1(e)(iii) and 4.1(e)(iv) and 4.3 above do not apply to International ESPs, but International ESPs must take reasonable steps to inform Subscribers that their local laws may prohibit or otherwise place limits on the sending of Spam, and that their local laws may provide certain rights to recipients of Spam.

4.5 Attached to this Code as Appendix A is a sample AUP fragment which sets out suggested clauses to deal with Spam related issues as required by this Code.

PART C – LAW ENFORCEMENT ISSUES

5. Law Enforcement Cooperation

5.1 Subject to applicable law, Service Providers will comply with all lawful requirements of law enforcement and regulatory agencies in investigating Spam activity.

5.2 Service Providers must ensure that they make available to the ACMA (or its authorised nominee) contact details (valid during normal business hours) of the person/team within the Service Provider who is responsible for addressing Spam issues. This contact point will be used as the central interface point for all Spam related issues involving that Service Provider - including requests for investigation, provision of Spam related information to the Service Provider and requests for information or technical intervention (eg taking action to shut down high volume Spam on the Service Providers' network).

5.3 Service Providers must ensure that they make available to the ACMA (or its authorised nominee) contact details (valid for all hours outside normal business hours) of the person/team within the Service Provider who can deal with urgent Spam related matters that must be addressed outside the process under clause 5.2. Such urgent out of hours action is expected to principally relate to requests to take action to, for example, shut down high volume Spam on a Service Providers' network where such Spam adversely affects the Service Providers' network, its customers and/or other parties.

5.4 For the purposes of clause 5.3 it will be acceptable for Service Providers to offer pager/call diversion arrangements in order to comply with the requirement for 24 by 7 contact availability. Reasonable contact/call back arrangements will be agreed with Service Providers consistent with their scale of operations and the probability of out of hours contact being required.

5.5 Nothing in clauses 5.1 to 5.4 above obliges an International ESP to do anything, or refrain from doing anything, if:

(a) that act or omission would result in the International ESP breaching the law of any jurisdiction other than Australia which is binding on the International ESP; or

(b) that act or omission would impose an undue administrative or financial burden on the International ESP, taking into account the obligations (if any) imposed on the International ESP by section 313 of the Telecommunications Act.

PART D – SPAM FILTERS

6. Making Spam Filters Available

6.1 Spam Filters must be offered either directly to Subscribers or via the provision of information in a reasonably prominent position on the Service Provider's Home Page regarding third party website/s that provide a means for End Users to have access to or acquire Spam Filters.

6.2 Where relevant, Service Providers are entitled to charge a reasonable cost for Spam Filters offered in accordance with Clause 6.1 such reasonable cost to be determined having regard to the nature, scope and functionality of the Spam Filter involved. Service Providers must advise Subscribers of any costs associated with Spam Filters at the same time as offering the Spam Filter.

6.3 Where a Service Provider provides client side Spam Filters direct to Subscribers the Service Provider must take reasonable steps to ensure that the Subscriber is advised at the point of sale methods by which the Spam Filter can be updated from time to time and further where information can be obtained regarding the continuing availability of the Spam Filter. Reasonable steps may include the provision of the information or a link to the information on/from the webpage from which the Spam Filters are offered to Subscribers.

6.4 When offering Spam Filters to Subscribers pursuant to this Clause 6, Service Providers must not offer that filter in a way that would involve a contravention of the "third line forcing" provisions, or any other provisions, of the Trade Practices Act.

PART E – SERVICE PROVIDER OBLIGATIONS

7. Open Relays and Open Proxies

7.1 ISPs must restrict inbound connections to any service they manage that allows email forwarding on behalf of third parties. Such restriction must limit access to the service to a closed user group relevant to the use of the application that the service facilitates.

7.2 ISPs must require their Subscribers to adhere to the same restrictions as are required of ISPs in clause 7.1.

7.3 ISPs must provide, in their AUP, a clause that allows for immediate account disconnection or suspension when the ISP becomes aware of inbound connections to any service they host that allows email forwarding on behalf of third parties, regardless of whether the open service is provided intentionally, through misconfiguration, or by other means not authorised by that third party including but not limited to through a Trojan horse or virus.

7.4 In the event of an ISP receiving notification of a Subscriber's system being responsible for the generation of Spam due to a breach of the ISP's AUP (which will contain the obligation to comply with the provisions of Clause 7.1), the ISP must take reasonable steps to notify the Subscriber of the breach and provide reasonable assistance, if requested, to assist the Subscriber to comply with the AUP provided however that in the case of a serious or continuing breach the ISP may exercise its powers of suspension or termination of the Subscriber's account as provided in the preceding clause. Reasonable assistance in this clause means the supply of information by the ISP in relation to the nature of open relays and suggested resolutions to the extent that the ISP can provide this.

7.5 ISPs should retain to themselves in their AUPs the right to scan within address ranges they have been allocated for Subscribers' misconfigured mail and proxy servers, and to suspend services to such Subscribers who fail to rectify such problems as found within a reasonable time period.

8. IP Address Information

8.1 ISPs directly responsible for the allocation of IP addresses to their Subscribers will use all reasonable efforts to retain information pertaining to those allocations for a minimum period of seven (7) days

9. Best Practices

9.1 Service Providers are encouraged to consider and implement best-practice actions that can be taken to assist in the reduction of Spam. Following are examples of practices and procedures that are currently being debated as best practice. These examples are not exhaustive or prescriptive as it is recognised that methods of generating and delivering Spam are constantly changing and therefore the best practices for dealing with Spam are also constantly changing.

Examples of Current Best Practice:

- *A Service Provider should publish SPF records compliant with the relevant Internet standards (see http://spf.pobox.com), for each domain administered by it, specifying its policies for the sending of email from that domain.*
- *A Service Provider will comply with all APNIC requirements in relation to the updating of WHOIS data including ensuring WHOIS data for any ISP customers is kept updated.*
- *ISPs should impose reasonable limits on the rate at which outgoing email can be sent by their Subscribers using an Internet account of the ISP, as determined by the ISP as being appropriate for the usual requirements of Subscribers to that type of Internet account.*
- *Any server on an ISP's network that is used for the sending of email, including servers of the ISP's Subscribers, should have a reverse DNS entry.*
- *ISPs should allow their Subscribers to authenticate to their mail servers using SMTP AUTH as specified in RFC 2554. Subscribers wishing to send email through the ISP's email server but who are not connecting through the ISP's network must be required to use SMTP AUTH or an equivalent mechanism to authenticate themselves.*
- *Where technically and commercially viable, operators of equipment (such as LNS or RAS hosts) which terminates user sessions with dynamically allocated addresses MUST cause such sessions' outgoing connections to be dropped where they are attempting to contact a remote host on TCP port 25.*
- *ISPs should not distribute Customer Premises Equipment (CPE) for connection to the Internet by their Subscribers that is so configured by default as to be susceptible to being remotely administered across the Internet.*
- *ISPs should control automated registration of email accounts so as to prevent accounts from being registered without direct human intervention.*

PART F – REPORTING SPAM

10. General Requirements

10.1 Service Providers must advise End Users how to report Spam which is allegedly being sent by:

(a) one of the Service Provider's Subscribers; or

(b) another Service Provider's Subscribers.

10.2 In respect of clause 10.1(b), the Service Provider's obligation is limited to notifying End Users that they should contact the other Service Provider (for example via its 'abuse@' email address) if they are receiving Spam which appears to be from a Subscriber of that Service Provider.

10.3 Service Providers must not impose any charges in respect of handling Reports from End Users.

10.4 Service Providers must maintain an 'abuse@' email address or other email address as notified by the Service Provider to allow End Users to make Reports.

10.5 Acknowledging Reports of Spam

10.5.1 (a) Service Providers may respond manually or use an auto-response to acknowledge Reports of Spam made to their 'abuse@' email address (or other email address as per 10.4 above).

(b) Regardless of whether an auto-response or a manual response is provided to the End User, the acknowledgement that the Report has been received must be issued to the End User within three business days of receipt of the End User's Report.

10.5.2 The acknowledgement to End Users must include:

(a) information on how the Service Provider deals with Reports of Spam that relate to its Subscribers;

(b) information, or a link to information, informing the End User about options for reducing the volume of Spam;

(c) information, or a link to information, about how the End User can Report Spam to another Service Provider (see clause 10.2);

(d) information, or a link to information, about how the End User can bring a Spam Complaint to the attention of the ACMA; and

(e) information, or a link to information, about the procedure by which an End User who is also a Subscriber of the Service Provider may escalate a Report about Spam into a Complaint.

10.6 The detailed obligations in clauses 10.1 to 10.5 above do not apply to International ESPs, but International ESPs must, in relation to Reports made by End Users located in Australia, treat those Reports in a manner no less favourably than Reports received from End Users located in the jurisdiction from which the International ESP provides its email service.

PART G – COMPLAINT HANDLING

11. Complaints from Subscribers about Spam

11.1 This section deals with the handling of Spam related complaints to Service Providers by their Subscribers.

11.2 ISPs and ESPs to whom the ACIF C547:2004 Industry Code of Practice on Complaint Handling applies must have regard to that code when dealing with Complaints about Spam.

11.3 All Service Providers must have and follow a complaint handling process which:

(a) has regard to AS 4269-1995 Australian Standard - Complaint Handling;

(b) is documented;

(c) includes the timeframes in which the Service Provider aims to investigate the Complaint, provide a final response to the Subscriber and escalate the Complaint internally (as required);

(d) allows Subscribers to be represented by an advocate or authorised representative when making a Complaint;

(e) provides for the recording of Complaints, the Complaint details and the outcome of the Complaint;

(f) provides for a formal response to be provided to the Subscriber of the outcome of the investigation of a Complaint;

(g) provides for internal escalation of a Complaint at the Subscriber's request;

(h) advises the Subscriber of further avenues of recourse in the event that the Subscriber is not satisfied with the manner in which their Complaint has been handled, or the outcome of the Complaint including but not limited to the Subscriber’s ability to refer the matter to the ACMA; and

(i) subject to clause 11.5, does not impose any charges in respect of handling Complaints from Subscribers.

11.4 A Service Provider's documented complaint handling process must:

(a) provide information in plain English;

(b) provide contact details for the Subscriber to make a Complaint to the Service Provider;

(c) specify the form which such Complaints should take;

(d) list further avenues of recourse that are available if the Complaint remains unresolved; and

(e) be provided to Subscribers upon request.

11.5 Complaint Handling Charges

11.5.1 A Service Provider must not impose any charges in respect of handling Complaints from Subscribers, unless the Service Provider can justify that the handling / investigative process for the Complaint is sufficiently onerous as to justify the levying of such a charge.

11.5.2 Where a Service Provider intends to charge a Subscriber for handling / investigating their Complaint, the charge must not be imposed without prior discussion with the Subscriber, which allows the Subscriber to decide to:

(a) pursue the Complaint and pay the charge;

(b) discontinue the Complaint; or

(c) pursue the matter via an alternate avenue.

11.5.3 Any Complaint handling charge imposed on a Subscriber must not exceed the total cost incurred by the Service Provider (for example, the cost to retrieve archived files).

11.5.4 Where the outcome of a Complaint is upheld in favour of the Subscriber, the Service Provider must refund any Complaint handling fees paid by the Subscriber for that particular Complaint within 30 days.

11.6 The detailed obligations in clauses 11.2 to 11.5 above do not apply to International ESPs, but International ESPs must, in relation to Complaints regarding Spam made by Subscribers located in Australia, treat those Complaints in a manner no less favourably than complaints regarding Spam received from Subscribers located in the jurisdiction from which the International ESP provides its email service.

12. Complaints Regarding Breach of the Code by Service Providers

12.1 Complaints may be made under this Code to the ACMA by a Service Provider about a contravention of this Code by another Service Provider.

12.2 Complaints by an End User about a contravention of this Code by a Service provider may be referred to the IIA or TIO from the ACMA under the power granted to the ACMA in section 514 of the Telecommunications Act, subject to the agreement of the IIA or TIO to accept the referral. Without limiting the grounds on which the IIA or TIO may withhold its agreement to accept a referral, the IIA or TIO may withhold its agreement where it considers that the complaint can be more conveniently dealt with in another forum or that handling the complaint may impose an unreasonable cost burden on the IIA or TIO.

PART H - MISCELLANEOUS

13. Date of Implementation

13.1 The current processes followed by Service Providers and the information they provide to their customers in relation to Spam vary widely. It must be recognised that the Code may require Service Providers to introduce changes to, inter alia, the way they respond to Spam Reports and Complaints; their AUPs, contracts, websites and other Subscriber information materials (including printed materials); the way they respond to law enforcement requests; the methods by which Spam Filters are provided to Subscribers; and the technical operation of their network. Staff training on the Code requirements will also need to occur.

13.2 In light of this, it is appropriate to provide a delayed implementation period for this Code. This Code will come into effect for implementation four months from the date on which it was first registered with the ACMA. Notwithstanding the foregoing Service Providers will use their best efforts to comply with the provision of this Code as expeditiously as possible.

14. Dates of Review

14.1 The full Code will be reviewed by the Task Force after one year from the date on which it was first registered by the ACMA.

14.2 The Task Force may decide to conduct an earlier review of the full Code or parts of the Code, if there is market-driven demand to do so. Membership of the Task Force is open to all IIA members including WAIA and SAIA who are associate members of the IIA. The review process will include consultation with consumer representative bodies and other relevant parties.

14.3 Any suggested amendments to the Code as a result of the reviews, will be submitted to the IIA Board for approval, and if approved to the ACMA for registration.

SCHEDULE 1 – LIST OF CONTRIBUTORS

Spam Taskforce

Allan Bell	Network Associates
Andrew Bedogni	Singtel Optus
Ana Tabacman	Singtel Optus
Mark Britt	NineMSN
Nina Ta	NineMSN
Peter Coroneos	IIA
Sophie Dawson	Blake Dawson Waldron
Jacquii Donovan	Brightmail
Patrick Fair	Baker McKenzie
David Graham	Sensis
Stuart Granger	Yahoo
Elizabeth Hastings	Telstra
Richard Keeves	WAIA
Andrew Kent	Messagecare
Kevin Karp	PPS Internet
Paul Kitson	Telnet Media
Jeremy Malcolm	WAIA
Tony Paterson	Cmon.com.au
Stavros Patiniotis	SAIA
Robert Pickup	Bluebottle
Mike Sadler	OzEmail
Mary-Jane Salier	OzEmail
Nicola Seaton	Webcentral
Ian Wilson	Vodafone
Paul Werner	Ozzieweb

The following organisations had the opportunity to comment on the Code prior to the Code being published for public comment:

ACMA
TIO
ACCC
Privacy Commissioner
Australian Consumers Association
CAUBE
ISOC-AU

APPENDIX A – AUP Fragment

SUGGESTED EXCERPT FROM A SERVICE PROVIDER'S ACCEPTABLE USE POLICY IN RELATION TO SPAM

NOTE: This document provides an example for Service Providers only. It is permitted, and indeed encouraged, that the content and wording be adapted for the Service Provider's specific purposes. In this example, "we" refers to the Service Provider, "you" refers to the Service Provider's Customer, and "Service" refers to the service provided by the Service Provider to the Customer.

X. SPAM

X.1 Definition

In this section, "Spam" includes one or more unsolicited commercial electronic messages with an Australian link for purposes of the Spam Act 2003, and derivations of the word "Spam" have corresponding meanings.

X.2 Acceptable use in relation to Spam

You may not use the Service to:

(a) send, allow to be sent, or assist in the sending of Spam;

(b) use or distribute any software designed to harvest email addresses; or

(c) otherwise breach the Spam Act 2003 or the Spam Regulations 2004 of the Commonwealth.

X.3 Our rights to suspend the Service

We may suspend our provision of the Service to you in the following events:

(a) if the Service provided to you is being used to host any device or service that allows email to be sent between third parties not under your authority and control; or

(b) if you are in breach of clause X.2 above;

provided however that we will first make reasonable attempts to contact you and give you the opportunity to address the problem within a

reasonable time period. What is reasonable in this context will depend on the severity of the problems being caused by the open service or breach referred to above.

X.4 Customer to minimise risk of breach

You agree to use your reasonable best endeavours to secure any device or network within your control against being used in breach of clause X.2 above by third parties, including where appropriate:

(a) the installation and maintenance of antivirus software;

(b) the installation and maintenance of firewall software; and

(c) the application of operating system and application software patches and updates.

Our right to suspend your account applies regardless of whether the open service is provided or the breach is committed intentionally, through misconfiguration, or by other means not authorised by you including but not limited to through a Trojan horse or virus.

X.5 Our right to scan for misconfigurations

We may scan any IP address ranges allocated to you for your use with the Service in order to detect the presence of open or otherwise misconfigured mail and proxy servers.

X.6 Our right to terminate the Service

If the Service is suspended and the grounds upon which it was suspended are not corrected by you within seven days, we may terminate the Service. In the event the Service is terminated under this clause, you may apply for a pro rata refund of any pre-paid charges for the Service, but we will have the right to levy a reasonable fee for any costs incurred as a result of the conduct that resulted in the suspension.