

## **BIAC BEST PRACTICES FOR EMAIL MARKETING**

**March 2006**

### **Background**

This elaboration of a set of voluntary best practices for email marketing is designed to provide guidance to online marketers so that they may adopt communication techniques which are at the same time spam-free and more effective. Such rules should make clear that spam has no role to play in legitimate marketing.

Most responsible organizations already follow industry codes or have adopted best practices. This document brings together a set of voluntary best practices drawing upon existing codes in order to provide all with a basis to using email for commercial or marketing purposes.

Increasingly, Internet service providers (ISPs) and email service providers (ESPs) are looking for ways to stop Spam by using filtering, black and white lists. As a result, they are inadvertently blocking legitimate email messages before they reach their intended recipients. The BIAC voluntary Best Practices for E-Mail marketing have been developed to aid business in ensuring that their own legitimate commercial email messages reach their intended recipients.

### **Intent**

BIAC's Best Practices for Email Marketing are a set of voluntary recommendations developed by business aimed at enhancing the legitimate commercial communications on the Internet in the fight against Spam.

BIAC proposes the following Best Practices Email Marketing as an important tool in combating Spam. As these Best Practices are voluntary, in all cases precedence is given to applicable legal and regulatory frameworks. As such, they are intended to complement existing laws that govern spam, privacy, e-mail marketing and marketing to children.

As suggestions of responsible business practices related to marketing, these Best Practices are meant to represent a global business view of responsible marketing practices that protect consumer interests while enabling needed business flexibility to service customer needs and explore new types of business opportunities. BIAC is cognizant of the fact that some national/regional legal frameworks or individual business practices may be more restrictive than those suggested. BIAC in no way suggests that these recommendations should be used where they may be less stringent than legally mandated requirements.

Given the rapid pace of technological change, they will be reviewed on a periodic basis to ensure that they remain relevant to the use of the Internet as a viable communication channel for legitimate e-mail marketers.

### **Recommended Best Practices**

- 1. The sending of electronic commercial messages should respect the consent requirements set by the national legislation in force in the country from which the marketer is operating, unless the marketer is knowingly and intentionally targeting consumers residing in another country.**
- 2. Organizations should keep records of opt-in/opt-out requests so that email lists can be cleaned prior to campaign broadcasts.**

Organizations should ensure that they have the means to honour opt-in/opt-out requests on a timely basis and to clean their lists accordingly.

An internal process should be in place that records proof of consent, when necessary, including the date and time. Additional records with respect to the consent might include originating Internet protocol (IP) address and location (including URL), where the address collection occurred and whether consent was obtained via another medium (e.g. business card, contest form, telephone, verbal communication or credit card [e.g. through a paying subscription to a list]). Organizations should be able to provide this information to a recipient upon request provided a reasonable amount of time has passed to permit database input.

- 3. In all marketing email (excluding transactional mail), recipients should be provided with an obvious, clear and efficient email or web-based means to opt out of receiving any further business and/or marketing email messages from the organization.**

In all email messages to current or perspective customers, organizations should include an opportunity for the recipient to opt out. This opportunity should not be buried in the email message and should, at minimum, be website- and/or email-enabled. The language used should be as simple as: "If you no longer wish to receive marketing offers from this organization, please **click here** or email **info@ABCcompany.com**."

The process for opting out should be simple and straightforward, and organizations should confirm by email or by website notice that the opt-out request has been or will be followed through without requiring further action by the consumer.

- 4. Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.**

The identification of the sender and source of the email should be clearly and obviously specified and, whenever possible, placed above the fold (that part of the email that is visible without scrolling).

**Example A: Direct from organization to subscriber**

Date: Tue, 5 Oct 2004 07:32:02 -0400; From: Bell Canada - Electronic bill [bill.presentment@bell.ca](mailto:bill.presentment@bell.ca)  
TO: JOE CONSUMER " [joe@consumer.com](mailto:joe@consumer.com) Subject: Your Bell e-bill is ready / Votre facture électronique est prête

**Example B: Third-party email service provider to subscriber on behalf of an organization**

From: "peteMOSS PUBLICATIONS <bounces@peteMOSS.com>" [v2user-13990-IxoyuP..CahrNet\\_0bkttg@mailier.whitehat.com](mailto:v2user-13990-IxoyuP..CahrNet_0bkttg@mailier.whitehat.com) Subject: SpamNEWS 07/21/04 To: [joe@consumer.com](mailto:joe@consumer.com) Date: Sat, 24 Jul 2004 18:50:17 -0700

Even in cases where the content is accurately related to the subject line, organizations are cautioned against using subject lines that refer to "free offers" or "winning prizes." This is, in part, due to the fact that some spam filters use keywords such as these to signal that the message is spam.

Email messages should include the sender's main postal address. All organizations are strongly encouraged to become familiar with the provisions in their national legislation of relevant countries that address this issue.

**5. Every email should provide a link to the sender's privacy policy.**

Organizations should make the information on their online information gathering processes readily available in one comprehensive privacy policy on their websites. The privacy policy could also include information or a link to opt-out of receiving future commercial communications.

**6. Marketers, list brokers and list owners should take steps to ensure that the addresses on their email lists were obtained legally.**

Some examples of reasonable steps that an organization can take to ensure clean lists include:

- Reviewing the privacy policy of the broker/owner of the list;
- Reviewing the procedures, if any, used to obtain the email addresses;

Obtaining assurance that the e-mail addresses were collected in a manner consistent with applicable laws. Having the broker or owner sign a contract warranting that they have complied with the requirements of privacy legislation.

**7. Marketers should use a high degree of discretion in sending email marketing to children and young people in order to be sensitive to the knowledge, sophistication and maturity of this audience.**

The ways in which those under the age of majority perceive and react to email marketing communications are influenced by their age and experience, and the context in which the message is framed. For example, email marketing communications that

are acceptable for teenagers will not necessarily be acceptable for younger children. The same applies for e-mail marketing of adult content, which includes material of a sexually explicit nature and material related to gaming and gambling, tobacco, alcohol, firearms and other weapons

For example, all email containing sexually explicit content should include the prefacing tag "SEXUALLY EXPLICIT", or such other language in the subject line..

While there is no way to guarantee the age of any person who signs up to an email subscriber list, When the content of an email is adult in nature, prior to sending the communication, efforts should be made to verify that the recipient is of age to legally receive and view such content Organizations should, therefore, use discretion and sensitivity when marketing to those under the age of majority, and should seek to engage parental permission in such communications. If a marketer is knowingly targeting a particular country, companies should consult any domestic laws or requirements related to parental permission and ensure compliance with them.

**8. Organizations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.**

Any complaints from individuals regarding the use of their email address should be dealt with courteously and within a reasonable time frame.

**9. Organizations may disclose the email addresses of existing consumers to third-party affiliates or within a family of companies if:**

- i. they are using the addresses for purposes consistent with their collection (i.e. for marketing related to the original purchase or to provide services related to that purchase);
- ii. there is an easy-to-use way to opt out of receiving further email communications.
- iii. or, if they have consent to do so;

When sharing email databases within and organization or corporate family, companies should keep in mind that consumers may not understand that different brands may be owned by one company or that different companies may be related and share e-mail addresses, and thus it should be transparent to consumers why they are receiving additional, related marketing offers (e.g. under a company brand).

**Technical Tips for Electronic Marketers**

**1. The following standard technical specifications are recommended to be adopted by sending parties:**

- All servers (e.g. inbound, outbound, websites) should have reverse Domain Name System pointer (rDNS PTR) entries in DNS records, the forward and reverse DNS lookups for the host should match, and the sending machines should HELO/EHLO with this name.

- Sender Policy Framework (SPF) or Domain-key (e.g. <http://spf.pobox.com>, and <http://antispam.yahoo.com/domainkeys>) records should be published by the senders and third-party sites associated with a mailing (e.g. websites, ESPs, etc.) and kept current at all times. Adoption of technologies that are similar in nature should be considered as they develop and become standardized.
- IP addresses that are distinct from other site servers should be assigned to outbound mail servers.
- WHOIS database records for all sender domains should be kept accurate and complete.
- Role accounts (e.g. postmaster@ and abuse@) should be functional and actively monitored for all sender domains, including websites, referenced in email content.

## **2. Senders should attend to bounce messages as follows:**

- They should promptly suppress "hard" (5xx — No such user / Mailbox unavailable, etc.) bounced addresses from all lists under their control when the total number of refusals surpasses three or more in fourteen days. If a 5xx bounce indicates spam blocking, the address may be reactivated if the spam block is removed.
- They should remove "soft" (4xx — Transient failures) bounced addresses when the total number of refusals surpasses five in consecutive campaigns from a single list, or five in aggregate from several lists within ten days.

Bounce-handling policies are explained in depth at the following sites:

- <http://help.yahoo.com/help/us/mail/defer>
- [www.isipp.com/standards.php](http://www.isipp.com/standards.php)
- <http://postmaster.info.aol.com/guidelines/bestprac.html>

\*\*\*\*\*

BIAC was created in March 1962 as an independent organisation recognised by the OECD as the official representative of the OECD business community. BIAC's members are the major industrial and employers' organisations in the 30 OECD member countries, representing over 8 million companies. Via its 31 standing committees and policy groups, BIAC mirrors all economic policy issues the OECD covers and examines their potential impacts on business in both member and an increasing number of non-member countries like Russia, China and India.