COUNCIL FOR RESPONSIBLE E-MAIL
E-MAIL DELIVERY BEST PRACTICES
FOR MARKETERS AND LIST OWNERS

The following recommendations were developed to promote best practices for marketers and list owners seeking to maximize delivery of communications with their in-house files of customers and prospects that have given their consent/permission to be contacted via e-mail.

Overview

The following recommendations were developed to help marketers better ensure the delivery of legitimate e-mail communications and build an ongoing, mutually beneficial dialogue with recipients through e-mail. These recommendations to maximize the delivery of email also assist in integrating marketing communications and securing brands in a significant and visible portion of the online space.

- They represent model practices that will help improve the likelihood of permission-based e-mail being delivered to the inbox and read by the intended recipient.
- They will also help relieve the burden being imposed on the Internet and on Internet Service Providers and Web-based email clients (hereinafter collectively referred to as "Mailbox Providers") by inappropriate and unwanted commercial e-mail.

Each of the following best practices and recommendations refer to marketers/list owners creating list(s) for their own use, or third parties employed by a marketer to provide this service. Each best practice and recommendation complements the next, and these practices should be taken into consideration as a collective entity.

Much has changed since the original release of this document in October 2003 – both in the technical world of e-mail delivery and with the creation of the Direct Marketing Association's (DMA) new Council for Responsible E-mail. This document represents an update of those earlier best practices.

BEST PRACTICES: INTRODUCTION

Marketers should give due consideration to matters concerning privacy, security, and confidentiality.

Marketers should be aware of and familiar with existing U.S. federal, state, local and international privacy and data protection laws that may govern commercial e-mail. DMA recommends that organizations consult independent legal counsel for advice with respect to specific facts and circumstances that may be applicable depending on jurisdiction and business practices.

Organizations are encouraged to refer to laws such as the CAN-SPAM Act of 2003, the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB) to evaluate if they are applicable.

DMA members should also comply with all self-regulatory guidelines of DMA. For best results marketers should reference other information from DMA on authentication, reputation, accreditation, feedback loops, tracking delivery, open relays or open proxies and bounce rates.

BEST PRACTICE #1:

OBTAIN PERMISSION

Marketers or List Owners should only send commercial e-mail to individuals with whom they have a pre-existing or current business relationship, or when consent/permission has been obtained. Marketers who implement affirmative consent permission practices accompanied by clear and conspicuous notice generally have higher response rates and lower complaint rates and blocking issues.

- **Inform the recipient about the nature of e-mail the individual will receive** and the frequency of those communications. The more specific the information about the type of offer or product, the better. Marketers/List Owners should also consider sending all recipients a confirmation or "welcome" message that reiterates this information (types and frequency of communications) and provides an opportunity for the recipient to opt-out of subsequent e-mails.

- **Create and make readily available a clear privacy policy** statement that is easily accessible to recipients, and explains what data is collected, how it will be used, or shared. Marketers/List Owners' privacy practices must be consistent their privacy policy/privacy statement.

- **Track and record all customer permissions** and the date and time received in order to expedite responses to inquiries.

Permission can be obtained in a number of ways. Forms of consent/permission include:

Affirmative Consent

Double Opt-in: A user has elected to receive e-mail newsletters or stand-alone commercial messages. A confirmation e-mail is then sent to the user to which he/she must reply (either by replying to the message or clicking on a URL contained within) before the list owner may add them to their list.

Confirmed Opt-in: A user has elected to receive e-mail newsletters or stand-alone commercial messages. A confirmation e-mail is sent, but user is not required to take further action in order to be included on the list. The confirmation e-mail includes the opportunity to cancel subscription.

Opt-in: A user has actively elected to receive e-mail newsletters or standalone commercial messages by checking an opt-in box. No confirmation e-mail is sent and user is not required to take further action to be included on the list.

Consent

Opt-out: A user is offered an opportunity to not be included on an e-mail list at either the point of collection (i.e, a pre-checked box) or in subsequent communications. A pre-existing or current business relationship may be established through proven online or offline contact, such as an application, purchase, transaction or request for information initiated by the individual.

Affirmative consent accompanied by clear and conspicuous notice provides a more highly qualified level of permission from recipients, which may help reduce the potential for spam complaints that could interfere with e-mail delivery.

- **Develop comprehensive and flexible online preference centers/registration pages** where e-mail subscribers can indicate and/or modify their specific interests and desires for content, frequency, and other pertinent information. Recipients should be able to easily change their preferences at any time they choose to do so, and have the opportunity to remove themselves from subscriptions or other e-mail lists. Marketers are encouraged to collect preferences for both online and offline campaigns, but only collect preferences that you intend to use.

- **Encourage customers and prospects to add the marketer's legitimate sending address to their personal "approved list/address book"** and provide up-front instructions on how to do so in registration pages. Benefits vary by Mailbox Provider, but may include special icon designation and full image content/link rendering.

- **Obtain permission for Wireless Domains carefully.** The CAN-SPAM Act mandates adherence to strict and highly specific notice and consent requirements for commercial wireless messaging. In addition, the Federal Communications Commission (FCC) and DMA maintain wireless domains suppression lists. This impacts ALL e-mail marketers, even if you do not intentionally engage in messaging to wireless devices. See Appendix B for a sample wireless registration page that complies with the notice and consent requirements.

BEST PRACTICE #2:

CONSIDER CONTENT

Recipients are increasingly labeling any e-mail communication that is not relevant or looks suspicious as spam. To avoid this misappropriation, marketers should carefully consider the nature of the recipient's consented interest, the content and presentation of the message and the quality of the pre-existing or current business relationship when developing offers or content. Marketers are reminded to review all content for CAN-SPAM compliance prior to deployment.

- **Communications should be relevant to the recipient and devoid of objectionable content**. Communications should only contain the type of content described in the notice the customer originally received and agreed to and should be relevant to their pre-existing or current business relationship.

- The **subject line must accurately reflect the message,** purpose and content. Marketers should avoid potentially deceptive prefixes in the "Subject" line, such as "RE" or "FW".

- A marketer's **brand should be prominent** in the "From" and/or the "Subject" lines. The marketer in the "From" line must be an entity who is "a Sender" of the message as defined by the CAN-SPAM Act.

- Marketers should **pretest creative elements and content** with anti-spam software to avoid words, phrases, coding, punctuation, and design common to spam.

- Marketers should **carefully balance the use of images and plain text.** Some Mailbox Providers currently "hide" all images by default. Therefore, make sure that every e-mail message contains a carefully considered balance of images and plain text. In particular, critical CAN-SPAM compliance features such as opt-out request functionality and your postal address should be visible to all potential recipients.

- The content should **clearly describe the offer and its benefits to the recipient**. Tips, special offers, and educational information based on each recipient's own behavior, interests, and needs often generate the best response rates and the lowers complaint rates.

- Marketers must include **a physical postal address** (Note: Compliance with DMA guidelines requires that this is not a PO box address, but a street address) in every e-mail. This address provides an additional channel for customer service and remove requests. Telephone or e-mail contact access for opt-outs may also be welcome by your subscribers.

- **Marketers must include a remove functionality** that offers a simple, cost-free, Internet-based and effective option that recipients can use to prevent future communications from the sender. All remove requests should be honored promptly and express to the subscriber how long it will take for their opt-out to take effect.

- **Provide a link to the e-mail preference center and privacy policy** in the footer of every message to allow recipients to opt-out and/or to update their e-mail address and interests/preferences.

BEST PRACTICE #3:

ASSURE DELIVERY

Mailbox Providers and other e-mail gatekeepers rely on a range of tools and techniques to block spam, including filters based on content, volume, and other delivery parameters. While policies differ by Mailbox Provider, it is essential for marketers and e-mail service bureaus to build direct relationships with Mailbox Providers and to follow established protocols and processes to ensure compliance and delivery.

- **Follow all delivery policies**, including acceptable use policies and "whitelisting" criteria established by Mailbox Providers.
    - An "acceptable use policy" is a document maintained by Mailbox Providers specifying the rules for sending e-mail into, and out of, their networks.
    - A "whitelist" is a list or process that some Mailbox Providers use to e-mail marketers to enter their networks without being subjected to certain (potentially stricter) levels of anti-spam filtering (e.g., volume filters).

- **Register for all feedback loops.** "Feedback loops" are a system whereby some Mailbox Providers share spam complaints with "whitelisted" senders in order to unsubscribe complainants from their lists. Feedback loops should also be used by marketers to identify and resolve high complaint e-mail campaigns and messaging streams emanating from their IP addresses/computer networks. In general, complaint rates (total complaints divided by total *delivered* e-mail) in excess of 0.1 percent can result in temporary or long-term blocks.

- **Implement compliance with authentication standards** including SPF and the Sender ID Framework immediately (for senders, compliance with both only requires the publication of SPF records). Also consider implementing more advanced cryptographic solutions like DomainKeys (and coming soon "DomainKeys Identified Mail"/DKIM)) Authentication compliance already is, or is expected to be, a component of all major Mailbox Provider delivery decision-making processes.
    - Please see the DMA/Epsilon Interactive Whitepaper, "Authentication, Accreditation & Reputation – For Marketers!" to learn how authentication is/will be used to enable more effective accreditation and reputation systems at Mailbox Providers. Visit www.the-dma.org/whitepapers.
    - Please visit www.emailauthentication.org for resources and tools for compliance with the latest email authentication standards.

- **Do not use the "bcc:" field** to address solicitations.

- **Monitor campaign delivery,** and open and click-through rates. A low open rate or high bounce rate may indicate a delivery issue.

E-mail Authentication

E-mail Authentication solutions verify that a computer server/IP address or a specified sender is authorized to send e-mail that purports to be from that sender and/or domain-name. Over the past year, a number of major Mailbox Providers have adopted authentication to better protect their users from spam and phishing and to reduce false positives (when legitimate e-mail is placed in the junk folder or not delivered at all) for legitimate e-mail marketers.

DMA is encouraging its members to comply with at least one of the currently available, complementary authentication solutions. These include IP-based solutions like SPF and Sender ID Framework (SIDF) and cryptographic solutions like DomainKeys and the forthcoming merged cryptographic authentication standard called Domain Keys Identified Mail (DKIM).

Compliance with e-mail authentication can protect your brand and customers by defending against spammers who feign legitimate corporate identities in their e-mails in an attempt to get through spam filters and scam recipients. In addition, compliance can help improve deliverability and reduces false positives. Leading Mailbox Providers that have implemented these solutions already have reported a reduction in false positives for compliant senders.

To date, the Internet Engineering Task Force (IETF), the Internet standards body, has not endorsed any one authentication method or program. However, SPF and SIDF were recently granted "experimental" status by the group, and DKIM was submitted for consideration as the cryptographic standard. It should be noted that it isn't unusual for industry to move forward with standards before the IETF completes it review and approval process, which can take years.

- **Review inactive customers** carefully and consider reconnecting offline with inactive customers who have previously granted permission. During this process, marketers should carefully monitor refreshed permission communications for complaints and delivery issues. It's best that attempts to refresh include the original permission date and time and remind recipients about what they will receive and how often.

- Use **separate IP addresses** for different types of messages. Separating marketing messages from customer service messages, bills, and newsletters will enable better management and intelligence on various communication types, with respect to complaints, delivery and problem resolution.

- **Time-and-date-stamp** each e-mail communication in the header or e-mail body to indicate when the communication was sent/received.

- **Monitor automated or inbound replies** to ensure timely response to customers and to track challenge-response notifications.

- **Audit e-mail infrastructure to ensure it is secure and there are no open relays/open proxies.** For up-to-date links to information on securing your server, visit www.ftc.gov/secureyourserver.

BEST PRACTICE #4:
HYGIENE AND SUPPRESSION

Sending e-mail to addresses that don't or no longer exist is considered by Mailbox Providers to be the hallmarks of spamming and poor marketing practices. Good list-hygiene practices help facilitate message delivery and are critical to developing consumer trust.

- **Develop a list-hygiene policy** that outlines the procedures which will be used to address such issues as:
  - format, syntax and domain errors
  - problem addresses such as role addresses (all@, admin@)
  - reply/inbound handling
  - processing of remove requests
  - handling of bounce-backs, including communicating unsubscribe time frames to each recipient, suppression of known invalid addresses, and address format validation

- The goals of the policy should be to:
  - minimize bounce rates
  - keep incorrect, incomplete, or outdated addresses to an absolute minimum
  - process online remove requests immediately and to process remove requests received offline within ten business days
  - tell those opting out how long it will take to be effective

This will set appropriate recipient expectations, thereby limiting the potential for complaints.

- Process and **suppress hard bounces** immediately.

- **Track soft bounces** to maintain list validity and suppress these addresses according to rules that support the sender's business and Mailbox Providers' recommended best mailing practices. A general rule is to remove soft bounces after three soft bounces.

- **Use all appropriate suppression files** including DMA's e-Mail Preference Service (a national list of individuals who do not wish to receive any e-mail solicitations), the DMA Deceased Do-Not-Contact List, DMA's wireless blocker, requests from call centers, Mailbox Providers, e-mail service bureaus, or from offline customer communications. The remove option should be in type that is easy to read and in a location that is easy to find. The best practitioners use research or focus groups to ensure that recipients are aware of and understand the remove options being offered.

- **Manage Wireless Domain** suppression carefully. The CAN-SPAM Act mandates adherence to strict and highly specific notice and consent requirements for commercial wireless messaging. In addition, the Federal Communications Commission (FCC) maintains a mandatory wireless domains suppression list. This impacts ALL e-mail marketers, even if you do not intentionally engage in messaging to wireless devices. To download the list, which under the law must be done on at least a once-a-month basis, visit: http://www.fcc.gov/cgb/policy/DomainNameDownload.html.

BEST PRACTICE #5:

EDUCATE STAKEHOLDERS

Marketers, list owners, Mailbox Providers, e-mail service bureaus and industry associations all share the responsibility for providing information and education to recipients about anti-spam tips, tools, technologies, laws, and industry programs developed to separate legitimate communications from spam.

- Promote the benefits of adding legitimate sending address to their **personal "approved list/address book**" on registration pages, e-mail communications headers and marketing materials. Benefits of being listed in the address book often include further delivery assurance of requested e-mail communications to the inbox.

- Encourage recipients to **use the provided remove/unsubscribe capability** to remove themselves from legitimate marketers' lists from which the customer receives legitimate, permission-based e-mail communications, instead of reporting these as "spam." Make the unsubscribe option easy to find and use.

- Show recipients **how to improve delivery** by their Mailbox Providers and provide information on adjusting e-mail filters on registration pages.

- Educate Mailbox Providers and recipients about **what is spam and phishing,** how to avoid falling victim to e-mail fraud and how to avoid falsely tagging legitimate e-mail as spam. An easy-to-understand graphical guide for consumers is available from The DMA online at http://www.the-dma.org/antispam/E-mail_Chart.pdf DMA has also partnered with the FTC to distribute *On Guard, Online*, a brochure offering consumers important tips for safe and secure electronic communications.

- **Talk to** Mailbox Providers about how their policies may sometimes conflict with federal and state regulations governing your industry including service messaging programs.

- **Communicate with legislators** and regulators about how current or proposed policies may affect your company. Information is available on DMA's web site (http://www.the-dma.org/government/) on specific legislative and regulatory issues, and how you can make your voice heard and be more effective in the policy arena.

BEST PRACTICE #6:

RESPOND AND RESOLVE

Marketers/List Owners and/or the e-mail service bureaus that send on their behalf share responsibility for handling any inquiries and disputes regarding e-mail delivery in a responsible and efficient manner that honors the individual's request and complies with existing and established guidelines for ethical business practices.

- Treat complainants **with courtesy and respect**. Remove complainers from your file immediately.

- **Cooperate** with list owners and Mailbox Providers to resolve complaints, as well as blocking and filtering disputes quickly and efficiently.

- **Provide individuals with information,** upon request, including when consent/permission was granted, or remind the individual of a previous business relationship (including details and the extent of that relationship).

- DMA Ethics Committees are interested in hearing from you if you believe a marketing promotion or practice is questionable and may warrant a formal review from the Committees. To **submit a potential case for Committee review** please follow this link (http://www.the-dma.org/guidelines/ethicscomplaintform.pdf) and download the form.

ABOUT THIS DOCUMENT

A cross-section of companies with in-depth expertise in e-mail and database marketing participated in the development of this document, which draws upon:

- *Eight Resolutions for Responsible E-mail*, developed by the Council for Responsible E-mail, part of The Direct Marketing Association's (DMA) Interactive Marketing Advisory Board.

- DMA's *Online Commercial Solicitation Guidelines*, which serve as a condition of DMA membership, as well as DMA's Anti-Spam Working Strategy.

These documents address standards for permission collection, content, unsubscribe and opt-out processes, third-party assurances, and suppression against DMA's E-mail Preference Service (e-MPS), a national list of individuals who do not wish to receive any e-mail solicitations.

Additionally, these new best practices include a discussion of authentication, which draws upon:

- DMA & Epsilon Interactive, *Authentication, Accreditation & Reputation – For Marketers!* (June 2005).
  http://www.the-dma.org/whitepapers/BI_DMA_AARWhitepaper.pdf

- DMA Briefing: *The Federal Trade Commission's E-Mail Authentication Summit* (November 2004).
  http://www.the-dma.org/cgi/dispnewsstand?article=3026

- DMA E-Mail Authentication Brief #2: *Authentication Coming This Fall: Do You Know Where Your E-Mail Comes From?* (July 2004).
  http://www.the-dma.org/cgi/dispnewsstand?article=2519+++++

- DMA E-Mail Authentication Brief #3: *Sender ID, SPF, and the FTC's Fall Summit* (September 2004).
  http://www.the-dma.org/cgi/dispnewsstand?article=2794+++++

APPENDIX A:

COUNCIL FOR RESPONSIBLE E-MAIL'S EIGHT RESOLUTIONS FOR RESPONSIBLE E-MAIL

CRE Members:

- Will not send commercial e-mail to individuals with whom they do not have consent/permission or a pre-existing or current business relationship.

- Must provide recipients of all e-mail solicitations with a clear, easy and effective method to unsubscribe, or in the case of some service message, i.e., billing reminders, information on how to remove themselves or unsubscribe from the service itself.

- Must not misrepresent the source of any message.

- Must not use false or misleading "Subject" lines.

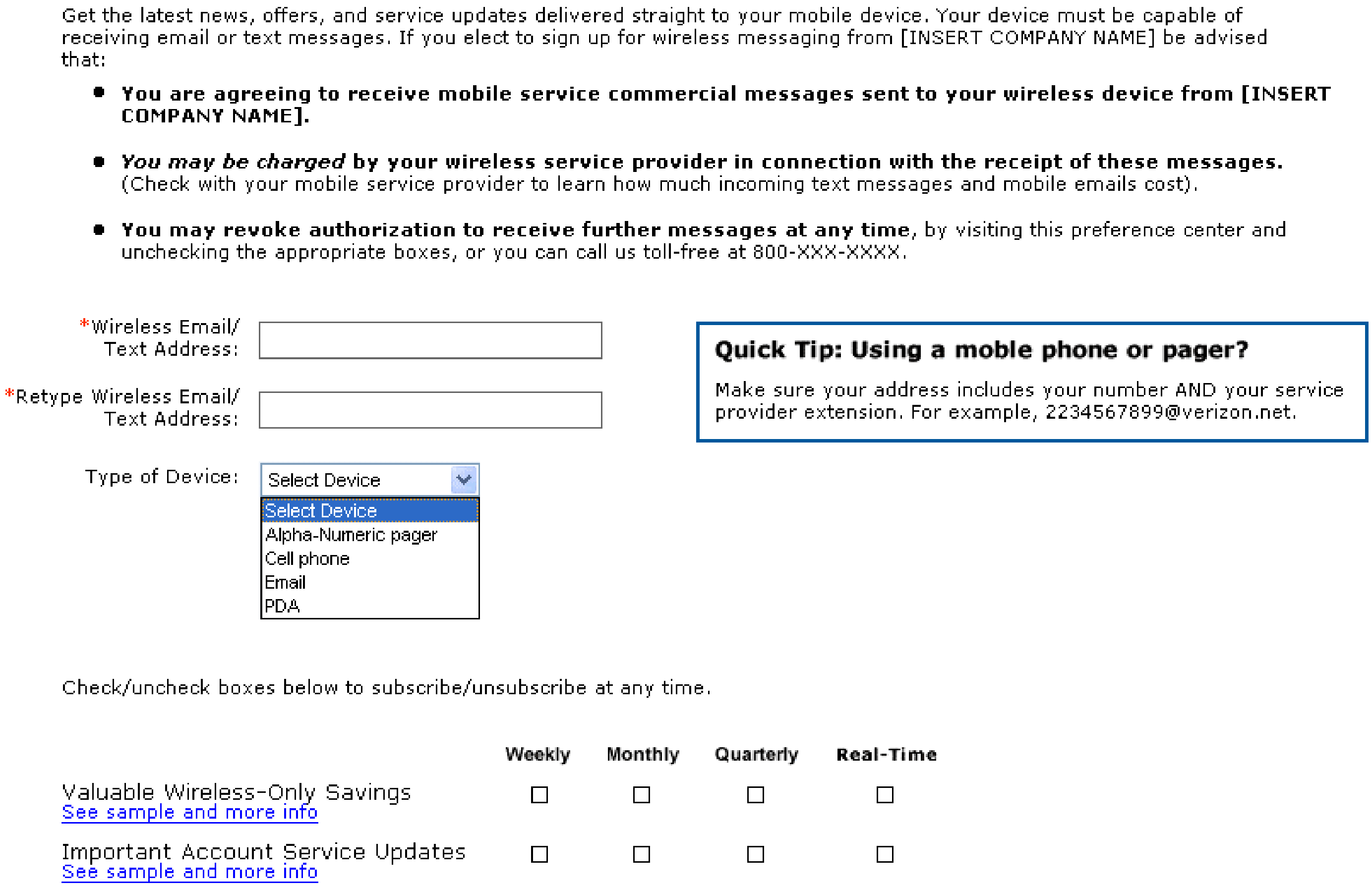
- Will inform subscribers about what personal information is collected about them and how it will be used before any such information is used.

- Must not harvest e-mail addresses with the intent to send commercial e-mail without the recipients' knowledge or consent/permission.

- Must not use dictionary attacks (send e-mail messages to random or systematically created e-mail addresses).

- Must not falsify the sender's domain name, use open relay servers or use non-responsive IP addresses.

APPENDIX B:
WIRELESS REGISTRATION PAGE SAMPLE



Get the latest news, offers, and service updates delivered straight to your mobile device. Your device must be capable of receiving email or text messages. If you elect to sign up for wireless messaging from [INSERT COMPANY NAME] be advised that:

- **You are agreeing to receive mobile service commercial messages sent to your wireless device from [INSERT COMPANY NAME].**
- ***You may be charged* by your wireless service provider in connection with the receipt of these messages.** (Check with your mobile service provider to learn how much incoming text messages and mobile emails cost).
- **You may revoke authorization to receive further messages at any time**, by visiting this preference center and unchecking the appropriate boxes, or you can call us toll-free at 800-XXX-XXXX.

*Wireless Email/ Text Address: ____

*Retype Wireless Email/ Text Address: ____

Type of Device: Select Device

Select Device
Alpha-Numeric pager
Cell phone
Email
PDA

Quick Tip: Using a moble phone or pager?

Make sure your address includes your number AND your service provider extension. For example, 2234567899@verizon.net.

Check/uncheck boxes below to subscribe/unsubscribe at any time.

	Weekly	Monthly	Quarterly	Real-Time
Valuable Wireless-Only Savings See sample and more info	□	□	□	□
Important Account Service Updates See sample and more info	□	□	□	□

APPENDIX C:
ADDITIONAL RESOURCES

DMA's Anti-Spam Webpage and Resources:
www.the-dma.org/antispam

TRUSTe Privacy & EU Safe Harbor Compliance:
www.truste.org/
europa.eu.int/comm/justice_home/fsj/privacy/

E-mail Authentication:
www.e-mailauthentication.org

U.S. Federal Legislation Search Engine
www.thomas.loc.gov

AOL Postmaster
www.postmaster.aol.com

MSN Hotmail Postmaster
www.postmaster.msn.com

Yahoo! Postmaster
help.yahoo.com/help/us/mail/bulk/bulk-01.html

Earthlink Postmaster
www.earthlink.net/about/policies/commercial/