WebSight Design, Inc.
3020 Bridgeway Ave., No. 317
Sausalito, CA 94965
HQ 415.331.8697 / Fax 415.332.1491

BULK MAIL CAMPAIGN RULES

No matter what you do, or how closely you follow the guidelines we provide, the issue of spam is an ever changing and always evolving problem – it is estimated that more than 70% of all email is now spam. Because of this, we can not guarantee that these guidelines are enough to ensure your mailing goes through or that new rules won't come into effect somewhere in the industry that catch you in the spam black-list vortex at some unknown point in the future.

Because of this, we highly recommend considering the use of third party mailing campaign companies such as Constant Contact (www.constantcontact.com). These companies do one thing – provide mailing campaign services for a living. As such, they are much better equipped to stay on top of industry rules, regulations and methods, and equally as important, have established relationships with the top service providers, who in turn have approved mailings that come from such sources.

If, however, you wish to maintain your own mailing solution, the following rules are the currently known rules as set forth by the US CAN SPAM ACT of 2004, as well as the top Internet Service Providers in helping to determine whether an email is deemed spam**.**

Due to the seriousness of the spam issue, no single rule can be overlooked.

1. Ensure email is sent in a way that only one recipient email address appears in the "TO" field. Many email programs include multiple recipient addresses in the "TO" field. This exposes each persons address to everyone else on the list and is considered potential spam. The same rule applys to the "CC" field.

2. Do not send blind emails. A blind email has an innocuous email address in the "TO" field (such as "clients@mydomain.com") and the actual recipients in the BCC field. While this allows your recipients to not see anyone else's email address, sending mass mailings using the BCC field is now considered as possible spam.

3. Every major service provider has their own threshold of how many emails can be sent at one time from their servers before you are considered sending spam, and another threshold for how many mailings can come from one source into their systems at a time before the source is considered as sending spam.

   Unfortunately these numbers change and when they do, service providers do not easily publicize this fact. Some providers will block you if they get 10 emails in one mailing, others block you if they get 200, 250, or even 500. Every provider is different and they routinely change their threshold.

Based on our experience, we recommend that you send out no more than 10 emails at any one time, at five or even ten minute intervals, and no more than 100 in any hour. Sending at any higher rate is strongly discouraged.

4. Send out no more than one mailing per week to the same list. Some industry experts recommend no more than two per month.

5. Provide an "Un-Subscribe" link to a web page on your web site that will automatically remove the recipient and give them a confirmation. This is a requirement – all mailings must have a clearly communicated "unsubscribe" link in them, allowing site visitors to have them removed from your list.

6. Many providers now require that you also allow recipients to simply reply to your mailing and state the word "unsubscribe" in the reply, upon receipt of which you are required to remove their address from your list. Therefore, the "From" email address must be a valid two-way address that is capable of allowing recipients to reply to that address.

7. In the body of the email, have a statement that the email was sent to "person@theirdomain.com" (the actual email address stated in your list). The reason for this is because many people have mail forwarded, and if they request to be unsubscribed from your list, may provide you an address not actually in your files, and this can lead to email being sent to someone who does not want to get it, thus potentially leading to your being reported as a spammer.

8. Include your physical mailing address. All mailings must have your organization's physical mailing address included.

9. Do not include large attachments in mass mailings. What exactly is considered "large" is an unknown factor due to the unwillingness of major service providers to reveal this information. As such, best practices would state that you send NO attachments, and instead, make related documents available on your web site, with a link to those documents in the email.

10. Only send email to those people who have specifically requested inclusion in your mailing list. Using "bulk mailing lists" or culling email addresses without the owner's explicit consent is now considered a first line spam tactic.

11. Using email addresses garnered from your own web site where the person filled out an online form but did not specifically request or give permission for mailings may result in complaints to their service provider without your awareness and if that occurs, you may be black-listed. Therefore, if you have obtained email addresses in this manner, it is suggested that you send out an initial mailing specific to the purpose of determining whether everyone on your list wishes to receive your mailings.

12. Send email as plain text or as a "Multi-Part" email. If you wish to send an HTML email, doing so without also ensuring that it includes a plain text version may result in your being black-listed due to the fact that most modern email clients (MS Outlook for example), by default, turn off HTML capability. This would result in your email not being readable by those recipients, some of whom may assume

that such unreadable code is spam and in turn report your email address to their ISP.

13. If you ever receive a bounced email in reply to your mailing, you must determine the cause – if it was blocked and marked as spam you need to find out why and correct the cause. This can often involve making simple changes to your mailing, while just as often, will require involvement of your email account provider. Occasionally, this can also involve dealing with third party spam black-list keepers, which can take months to resolve.

    If an email comes back due to a "full" mail box, it is highly suggested that you keep track of such addresses, and after the 2nd failed mailing to that address, to remove it from your list, however this is purely for the purpose of ensuring that you maintain a high quality list.

14. If an email comes back because of a "permanent fatal error", you can remove it from your list, however, if it comes back because of "unknown recipient" or another similar reason, it may be a sign that you may have a bigger problem with your email account provider. Getting one or a small handful of "unknown recipient" returns is not unusual. Having this happen repeatedly requires contacting your provider because the root cause may in fact be related to your mail provider's "A record" or "MX Record" settings and is a potential red-flag issue for some spam watch organizations.

15. Upon receiving an unsubscribe request, immediately remove the address from your list – all it takes is one unintentional additional mailing to someone who has requested removal to have your email host black-listed. The U.S. CAN SPAM law of 2004 actually allows you ten days, however even if you remove an address within that time-frame, if you've sent out a 2nd mailing after getting the removal request, a report to that recipient's ISP may still result in your being black-listed, then having to fight to get off of the black-list.

16. If you are making a product offering or purchase solicitation through the mailing, you must clearly state that this is the case – the CAN SPAM act states that this must be in the form of the word _Advertisement (with the leading underscore) and this needs to be located above the promotional message or at the top of your email.

17. Do not include mis-leading or false header information, subject lines or content.

18. Steer clear of potentially spam-like subject lines.
    a. Never use ALL CAPS
    b. Never use exclamation points!
    c. Keep subjects to 49 characters or less (including spaces)
    d. A popular technique of spammers is to include a recipient's name in the subject line – personal names therefore in this field are potential spam flags

19. Avoid spam-like content in the body of your mailing
    a. Never use ALL CAPS
    b. Avoid excessive use of "click here", $$ and other symbols

c. Avoid words like "free", "guarantee", "spam", "credit card", "sex", etc.
d. Do not include unsubscribe instructions more than one time in an email
e. If you use an automated mail-merge solution, the potential exists for a mistake to be made where, instead of their name, it shows the mail-merge code and this is a major spam flag. Alternately, having Dear , (where the name is missing) is not only bad form, it's another potential spam flag so if you DO use mail-merge, double check the results output and resolve such issues before mailing.
f. Do not use all or extensive **BOLD lettering**
g. **Do not over-use multiple color font variations**

20. Establish a strong consumer-favorable privacy policy, post it on your web site, and refer to it in your email.

21. Ensure that all links in your email match the domain name of your "From" address. For example – if your mailing comes from news@yourdomain.com and you have a link in your email that goes to www.someotherdomain.com this is a conflicting use of domains.

22. Ensure that no links in your email use numeric IP addresses. For example, the web site www.cnn.com is really located at http://64.236.24.12 (named domain addresses are in fact just aliases or masks for the numeric address) HOWEVER – for anti-spam rule following, having numeric based links in an email is one possible spam factor.

23. Never mask a link in your mailing. When creating an html based email you would often type a link like this

    www.mydomain.com

    One of the biggest scam techniques used nowadays is to do something like this instead:

    www.mydomain.com

    Note in the 2nd version how the URL inside the href tag is different than the one to it's right. – This is now done by people who want to deceive recipients, because an HTML email will not show the code to the left – in both cases above, the recipient would normally only see www.mydomain.com

    This is mentioned in this document because you may
    a) Unintentionally mis-spell one of the two references
    b) Have some notion about marketing that allows you to think deception in this case is minor and therefore acceptable.

    The fact is, this technique is deemed "phishing" and is actually a crime.

24. Use a separate stand-alone email address for your "from" field – set up specifically for your mailings. This way, if your mass-mailing is flagged at some point by one or more ISP, as spam, you are more likely to still be able to send email from your other, more vital email addresses. Ideally, it would be a best practice to have a separate domain name set up just for the purposes of sending

mailings, because the potential exists for an entire domain to be blocked once an email is black-listed (as compared to blocking just one email address).

REFERNCE MATERIAL:

FTC www.ftc.gov/spam

U.S. CAN-SPAM ACT
http://thomas.loc.gov/cgi-bin/query/z?c108:s.877.enr:

U.S. State by State laws regarding Spam
http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm

Google GMail Rules
http://www.google.com/mail/help/bulk_mail.html

Hotmail Anti-Spam policy
http://privacy.microsoft.com/en-us/anti-spam.aspx?HTTP_HOST=privacy2.msn.com&url=/anti-spam/en-us/default.aspx