Email Deliverability Guide

Most email marketers are concerned that their email practices may result in being blacklisted as a spammer which could severely impact their marketing campaigns especially if a single email server is used since blacklisting is essentially IP based. Blacklisting can result if an ISP perceives you to be a source of email spam which is unsolicited commercial email. Blacklisting is the worst case scenario for email marketers along with email spam filtering to “junk” email boxes, rather than delivery to the inbox.

In this guide we’ve included some best practices to avoid this happening to your email communications along other information:

- What are the best practices and tips for getting your email delivered
- Monitoring reports and blacklist sites
- Technical Infrastructure requirements and options

How do I get my email delivered? What are the best practices we should be following?

1) **Give the Reason** - Indicate why your customer is receiving it. For example, "You are receiving this email because you selected the option to receive our monthly newsletter when you purchased a product from us. Use profiles to capture the source and date of their opt-in in order to personalize your message.
2) **Give them an Out** – Give your customer an easy and quick way to opt out of receiving future communications. For example, "If you would no longer like to receive our newsletter, please click on this link to unsubscribe or reply with “unsubscribe” in the subject line”. Keep in mind that people will decide to label an email as spam in less than a second. If it is not easy and quick to find the opt-out link, you increase the probability of being labeled a spammer.
3) **Use a Known Email Domain** - Sounds obvious, but we know from the emails we receive that it's not. If customers opted-in to your newsletter while purchasing a product from joes-widgets.com, then an email from sams-building-supplies.com is more likely to be reported as spam, since they don't recognize the latter domain as a business they have used in the past.
4) **Keep the Trust** - Trust is arguably the number one issue in eCommerce. Provide a link to your privacy policy in your email or include on the bottom of the email, and if you belong to a trusted organization such as the Better Business Bureau, consider placing the trust seal in the email also.
5) **Ensure Value** - If your emails contain information that the customer finds of value, you will reduce the risk of getting placed on an email blacklist. If you don't have much value to communicate, don't send the email!
6) **Watch the Frequency** - Don't send emails too often (in your customer's opinion!). Weekly or even monthly communications may be considered too frequent for some types of communications, while daily may be acceptable for others. Yearly communications sometimes result in customers forgetting they did business with you, and may increase the likelihood of being reported to an email blacklist. Promotional messages should usually be sent less frequently than informative messages (e.g. product sales vs. daily stock market reports).
7) **Ask for Feedback** - In your emails, ask your customers for feedback on the value of the email content, and any suggestions they have for improvement. If you ask for feedback, however, be sure to reply to it. Ideally, feedback receives a personal reply. At the very least, however, you should have a feedback box with an automated reply. Remember, though, that feedback that appears to be ignored can upset customers which can cause attrition or email blacklisting. Some customers may try to unsubscribe by using the feedback address or link, rather than the unsubscribe link. If you don't want to be on an email blacklist, you MUST monitor and quickly address any complaint messages or requests for removal. Otherwise, your next email is likely to be reported as spam. Tip – use MarketFirst surveys to aquire feedback. Net Promoter Score (NPS) is an excellent program to find out how customers really feel about your products and service. Contact Meitasoft to learn more.

Meitasoft Inc. All Rights Reserved 1/14/2010

8) **Allow Personalization** - As possible, make it easy for people to change the email address that you use for communications, and select which types of information they wish to receive.

How to I gain permission?

Use all the media -- both online and offline -- that you already use to interact with your marketplace successfully, such as:

1) Direct Mail: gather opt-ins by using postal postcards or other direct mail packages to ask people on your postal list to opt-in to your email list. Direct recipients to a Web form where they can sign up. 1/3 of email address will change within a year so encourage people in your mailings to update their information by clicking on a link to a web form.

2) Broadcast Email: Using a rented list is not encouraged, but if you must be very sure the email list you use is either an opt-in list (or double-opt-in to be safest.) Avoid using rented lists if a list owner can't prove it's an opt-in list.

On occasion if you have a very strong, brand name, and you have an email list of customers who have interacted with you recently (within 1 year) you may be able to get away with sending a broadcast email to those customers once to ask them to opt-in. This may not be legally safe in Europe or Canada, and unless you are careful, it can hurt your brand in the USA. So proceed with caution.

3) Email Newsletter Ads: Many marketers have had great success gathering qualified prospect opt-ins by advertising in email newsletters because newsletter lists are often more targeted than broadcast email lists. You won't have much space, sometimes less than 50 words, so focus your copy on a single strong offer. White papers, free newsletters, sweepstakes and other free offers work well.

4) Your Communications Materials: Your opt-in offer should be on almost every communication your company makes. This includes, every page of your Web site (consider making it part of your navigation bar), business cards, employee email signatures, space advertising in magazines, print materials, order forms, customer service in-bound calls, etc. Remember a few years ago when you had to add your URL to everything? Now you have to do the same with your opt-in offer.

How Long Does Permission Last?

People have short memories. The general rule of thumb is any name you haven't emailed in six months to a year has probably forgotten they ever gave you permission. So if you email them, they may think you're a spammer.

This means you should take two steps:

1) Have a plan of action for the opt-in names you collect. With their permission you might want to email them some sort of useful information at least every 4-6 weeks. Quarterly mailings are probably too far apart.

Meitasoft Inc. All Rights Reserved 1/14/2010

2) As mentioned in the previous section, try to add a section to your messages that tells people how you got their email address, and how they can get off the list easily (and without cost.)

Marketing Scenarios – Spam or not?

1) Q: "We have close to 250k users who subscribed to our financial services, but yet we have never emailed. The 250k are users who used our site maybe 2/3/4 years ago before we even had a regular newsletter, and have either never returned, or have no idea we still exist. Should I:
   a. Send them a one off email stating 'hey remember me, look at me now I've grown and can help you now in your every day finances like never before etc..."
   b. Just add them to our regular news alert and hope for the best
   c. Send them an email asking them permission for me to send them emails in the future. (maybe a form within an email)

   A: If you are absolutely, positively sure these folks opted in to get a regular email (i.e. If you've seen the opt-in form with your own eyes) then you can email them. However, someone who opted in four years ago (or even four months ago) has probably forgotten they ever gave that permission. Some marketers would go so far as to consider it rescinded. Suggestions:

   - Dump the oldest names. Anything older than 12 months probably isn't any good anymore, even if you were to email them. According to research, every year about 1/3 of people on your list change their email address. So although you think you have 250k names... you may really have up to 250k bad addresses!

   - If you can divide the newer names by month they came in, you could create a special, one-time-only campaign with a very strong offer for everybody older than 6 months. In that campaign you might want to very honestly start out saying, "You registered for our newsletter in May 2009 and we're very sorry to have kept you waiting for so long. If you are still interested, then please ...."

   - Start sending everyone 3 months or newer the newsletter on a regular basis from now on, being sure to include an "opt-out" (how to unsubscribe) line in every single issue.

   - Use an auto-reply message to your opt-in collection campaign now so when someone opts-in they immediately get a welcome message in reply that lets them know when to next expect an email message from you.

2) Q: Would it be considered a bad practice to send out a mass mailing to people who have once visited your site, and either bought something or not, but didn't sign up for any type of opt-in list etc.? In the future we are planning to add an opt-in form to the site to avoid this problem.

   A: The only time you should email a buyer from your site without any sort of permission is when it's in relation to their specific order. There is only one exception (purists might not agree): You might be able to get away with one single email sent to buyers who would definitely remember doing business with you. For most companies that would mean very recent buyers. This could be

Meitasoft Inc. All Rights Reserved 1/14/2010

a thank you note with an offer to opt-in to receive special offers in the future. However, this should be a one-time affair for your company. Once your site is set up to collect opt-in permission from buyers and visitors, you should never, ever send an unsolicited mass email again.

3) Q: Is it acceptable to send one uninvited e-mail to a prospect and simply tell them who you are and why you are contacting them and tell them that they won't hear back from you, unless they opt-in to do so?

   A: Nope, you shouldn't send out spam to avoid sending spam in the future. With spam, once is too many times. You should use other tactics to collect e-mail addresses: *Passive tactics*: Add an opt-in to every page of your Web site. *Aggressive tactics*: Telemarketing; direct marketing; ezine advertising; co-registration, renting permission-based lists to send email to (always ask for proof in the form of the list that members opted-in on).

4) Q: If I do an email blast to the last year attendees of an event my company has produced announcing this year's event, is it spam?

   A: Technically yes, if the recipients didn't say 'Let me know about next year's event". However, if you have a very strong brand name, you may be able to get away with it just once. Repeated blasts should be out of the question. You might want to make sure of two things:
   a. Make your offer compelling so that the maximum people will click through and you can collect their names for future email. Instead of a paid reg form, you could do a free "send me more info" form. Plus, let people know this will be the ONLY time they'll get this offer. A safer alternative might be to hire a telemarketing team to call last year attendees to ask permission for future mailings.
   b. This year, add a line to the reg form asking if you can alert them about future offers, so you don't have the same problem in the future.

5) Q: Is it ok to Email lists from Business Events you attended?

   A: Not unless they specifically opted-in for what you are e-mailing them about.

6) Q: How do I get my e-mail through corporate spam blockers/filters?

   A: One of the side effects of spam filters is that legitimate e-mail often gets blocked, and many marketers have seen their click-through rates drop. ISPs use different filters, and IT departments of corporations often add additional filters. Each filter uses different criteria for determining which e-mails are spam, so getting through filters becomes a very difficult task, particularly since filters constantly evolve. However, while various filters define spam differently, legitimate email marketers should do the following:
   - Avoid 'trigger' words, such as 'free', 'no cost', and 'win'.
   - Avoid subject lines with 'order now', or 'sale', and messages with many exclamation marks and question marks, and multiple fonts.
   - Make sure the content of the email matches the heading in the subject line because spammers typically manipulate headings so that the e-mail looks like it's coming from someone it's not.
   - Make sure that the subject line includes several words that also appear in the main body of the email.
   - You should have a relationship with the ISPs, filter suppliers and blacklists so that they can advise you on crafting acceptable e-mail messages, and identify the domains that return e-mails as 'undeliverable'.
   - When sending out an e-mail message, register at least seed names with each ISP so you can see how your content is portrayed through

Meitasoft Inc. All Rights Reserved 1/14/2010

each portal. If your emails aren't getting through with certain seed names, you can then contact the ISP and find out what is going on.

- Test your email content against free or low cost spam filtering test sites: New! Mail Server Test Center (MSTC) or down load Spam Assassin and run messages through this service to see where there are problems.
- Encourage your customers to develop 'white lists', for example your customer could have their company's IT department place your company's name on the white list and have your e-mail pass through the proprietary filter. Adding your "from" address to their contact list and email client white list will help ensure your email is delivered to their inbox. Here are instructions for people to follow to add you to their white lists http://www.sitesell.com/whitelisting.html
- A double opt-in might also increase the likelihood of your messages getting through – single opt-in email often gets filtered out as spam simply because it is sent to the wrong recipient.
- As mentioned earlier, remove old (>1 year) inactive subscribers; Inactive subscribers are most likely to mark your email as junk. Sure, nobody wants to willfully shrink the size of their opt in list, but you have to think long term.
- Consistent timing for large mailings (a blast of >5K to a sinlge ISP) ; ISPs love it when you consistently send email blast on the same day at near the same time. Since spammers don't care, consistency is the mark of a responsible email marketer. Tip - Use a platform like MarketFirst to schedule sends at a specific time. Also think about your process and send event or trigger-based messages - a survey on a new order or a reminder one month before an expiration or scheduled event.
- Send in spurts; Some ISPs have limits as to how many emails you can send to in a given period of time. If you're having trouble sending email to a particular ISP such as Yahoo, Gmail, or Hotmail, break your list up into smaller lists or use segment your audience into smaller groupings and use it to control the flow rate.

7) Q: How do I distinguish my e-mail from hundreds of others?

A: If the recipient has opted-in to your communication, they will be expecting it and looking for it. Make the subject line relate to the offering that they are expecting.
Make your company/brand name clear. Foster loyalty in all your marketing activities to make customers want to open your e-mail.

How do I know if I have an email deliverability problem?

Test your emails with "seed mailboxes" (2-4) that you set up with the major ISPs (hotmail, gmail, yahoo, and AOL. Did you receive the email? Monitor your MarketFirst reports looking at "failure" counts. This is could be an indication that your list needs attention or your content is scoring high with spam filters, or you've been blacklisted. Hard bounces i.e bad email address, should be marked as Unsubribe immediately.

We often get the question: "How do I know if my company is on a SPAM Blacklist?" Followed by "If my company is on a SPAM blacklist, how the heck do we get unlisted?

There are several hundred SPAM blacklists but luckily, there are a few tools that can help you check most of them quickly. We've included here a handy reference with the sites that you can use to check your blacklist status. We've also highlighted a couple of the more prominent SPAM blacklists.

Meitasoft Inc. All Rights Reserved 1/14/2010

Blacklist Monitoring and Status

Most SPAM blacklists track the reputation of the email servers that are being used to send outgoing email for your domain. Some SPAM blacklists track more than IP's – they also track domains, URL's and a few even create a unique 'hash code' based on the content of the email. If their systems see more than a few dozen emails with an identical code – meaning dozens (or more) of identical emails, they'll list the specific email content as SPAM.

Here are 4 sites where you can check multiple public blacklists if you know your servers IP address(es):

- **http://www.mxtoolbox.com/blacklists.aspx.** MXToolbox is free. Enter the email service IP addresses and mxtoolbox checks about 100 blacklists.
- https://www.senderscore.org/
- **www.dnsstuff.com.** DNSStuff is an inexpensive (almost free) service where you can check 97 blacklists. Includes other DNS and network tools too.
- **http://www.dnsbl.info**. (Domain Name System Blacklist). Free service. Checks about 80 blacklists.

If you find that you have been blacklisted begin the process of contacting each of the blacklist services and find out the process for getting your IP removed.

Commercial monitoring solutions

Companies like Return Path (www.returnpath.net) and Delivery Monitor provide reputation and alerting tools. Return Path is the heavy weight is this industry. They offer monitoring tools and services that show you exactly where your email is going with every campaign, what it will look like when it gets there and which factors will impact your delivery rates at the various ISPs. Armed with this information, you can improve your response rates. Their "Gold" offering includes:

- Reputation Monitor
- Campaign Preview
- Mailbox Monitor
- Blacklist Alert

Delivery monitor is lighter weight and a less expensive delivery monitoring provider http://www.deliverymonitor.com. In essence, you are provided access to a series of email addresses. You add these addresses to your list. The service will then tell you whether your message was blocked, made it to the junk or bulk folder, or to the inbox. You can then use the tools to aid you in improving your delivery rates. There are more sophisticated services, but Delivery Monitor will give you a good starting point.

Certification (also called accreditation) is important. Since transactional mail is important in your business, you may want to look into having your mailing practices certified and also have your mail server white listed with Yahoo! and AOL. Yahoo! will want you to be running closed loop verified (aka double opt-in) mailing lists. You can find the details by visiting the help section for bulk mailers on the Yahoo.com web

Meitasoft Inc. All Rights Reserved 1/14/2010

site, under the sub-domain help.yahoo.com. Also, you should be white listed with AOL. Go to the postmaster page for AOL for the details.

A few other blacklists deserve "special mention":

Spamhaus.org. (www.spamhaus.org)

SPAMHaus.org's mission is to rid the world of unsolicited commercial email ("UCE") by creating and monitoring a network of thousands (millions?) of 'spam honeypot' email addresses. These are email addresses that are expired, or that never were 'real' recipients that Spamhaus acquires from ISP's. They 'plant' the addresses on various websites around Etherspace. Since these are not 'real people' – the addresses should never end up on an opt-in list, so if you send an email campaign and it ends up in one of Spamhaus' inboxes – clearly your list development practices are not cool. [Note: Some list vendors develop emails lists - albeit illegally - by scraping websites for email addresses. This is why you should never us these lists].

Spamhaus then adds the sending email servers to their blacklists. Overall it's a pretty good system but not flawless in our experience. For example, if you are capturing registrant information from your website or from online events, an ill-willed smart-alec can enter a bogus / honeypot address into your list. Your well intentioned campaign gets caught and viola – you are on Spamahaus' list. Solution: Always use double opt-in processing (most email services providers like Pinpointe provide mechanisms to enforce double opt-in when using their forms to collect subscribers).

UCEProtect (http://www.uceprotect.net/en/rblcheck.php)

UCE Protect deserves mention because its one of the few major SPAM blacklists where you can blacklisted because of something someone else did. UCEProtect monitors and tracks the SPAM reputation of individual email server IP addresses, and factors in the reputation of other servers in the same network as well as servers hosted by the same ISP. UCEProtect's 'guilt by association' approach means your servers can be blacklisted if your ISP hosts other systems that are caught for SPAMMing.

Uribl.com (www.uribl.com)

URIBL uses 'SPAM honeypots' – just like Spamhaus.org does. The difference (we believe) is that URIBL will keep the URL (or domain or sending email address) of the offending domain on their list for an undefined time — until any (offending) traffic stops and you clear your domain with URIBL by confirming that the offending problem has been fixed.

Microsoft Frontbridge (88.blacklist.zap – not a website)

If you find your emails are getting blocked by recipients who are using Outlook, then you may want to review your MTA logs (email server logs) for references to 88.blacklist.zap. That's Microsoft's internal Frontbridge SPAM filter service that is used to protect aanyone using Outlook, and who has their email configured to use Microsoft's spam filtering service (which is free). If you have stumbled onto Microsoft's blacklist Your email server log will include an entry such as "550 Service Unavailable; host [xx.xx.xx.xx] blocked using 88.blacklist.zap. Please forward this message to delist@frontbridge.com. Response time is within 24 hours.

Enterprise Firewall SPAM Blacklists

Meitasoft Inc. All Rights Reserved 1/14/2010

Companies that make SPAM firewalls each maintain their own network of systems that share SPAM information. All of them track results based on IP address; several also track history based on URLS within emails, the sending domain and sending email addresses. The most common Enterprise SPAM firewall companies and their respective SPAM databases are summarized here:

Vendor	SPAM Database / Repository	IP Address	Links/URLs	Domain	Other
Proofpoint:	https://support.proofpoint.com/rbl-lookup.cgi	YES	NO	NO	NO
Cisco / Ironport:	http://www.senderbase.org	YES	NO	NO	NO
Fortinet:	http://www.fortiguardcenter.com/antispam/antispam.html	YES	YES	YES	YES
Barracuda:	http://www.barracudacentral.org/lookups/ip-reputation	YES	NO	YES	NO
McAfee:	http://www.trustedsource.org	YES	YES	YES	NO
Sophos:	http://www.sophos.com/security/ip-lookup	YES	NO	NO	NO
Symantec:	http://www.symantec.com/business/security_response/landing/spam/index.jsp				

Sender Setup and Sending Infrastructure Requirements and Tips

Make sure you are sending from a dedicated IP address. Note that it's possible to have a number of domains pointing to the same dedicated IP address. Anti-spam identification protocols like SPF/SenderID and DKIM are IP based. The IP addresses should have proper reverse DNS look ups. Why? Spammers tend to hide their identity. Since you are a legitimate bulk mailer, you want to identify the source of your mailings. Also, since a lot of spam comes from residential IP addresses, bulk mail from these sources tends to get dropped.

Minimally published a sender policy framework record (SPF). Some networks are using SPF records to verify whether a bulk mailer's mail stream should be white listed or black listed. If you are not familiar with SPF and how to publish an SPF record, you may find this article of value. You will find links to the formal protocol, along with resources put together by Microsoft and a wizard to aid you in publishing a record.) This can have a bearing on whether your mail is accepted. Additionally consider deploying DKIM. DKIM is an emerging e-mail authentication standard supported by Yahoo, Google and others ISPs, as well as a growing number of Email Service Providers that was developed by the Internet Engineering Task Force. DKIM allows an organization to cryptographically sign outgoing e-mail to verify that it sent the message. Deploying DKIM for your company is pretty straightforward. If you are managing all of your own email servers and outbound email, including sales, marketing and transactional emails, there are 4 steps that can be found here http://www.itworld.com/software/67334/how-deploy-dkim-email-authentication-4-steps

Join feedback loops; Feedback loops allow you to see who is marking your email as spam (so you can remove them). Some ISPs, like AOL, provide an easy way to join the feedback loop. For other ISPs, you may need to contact your email service provider to see if they can provide you with this information.

Meitasoft Inc. All Rights Reserved 1/14/2010

The SMTP mail “from” address must be a valid email address. When sending email, the sending server connects to a receiving email server. The sending mail server issues a series of commands. One of these commands is to provide the receiving server with the SMTP mail “from” address, which is used to send notices about bounces and so forth.

The domain in the SMTP mail “from” address needs to match the domain in the EHELO/HELO address. This can be important. Also, does the domain in the EHELO/HELO address properly identify your mail server? Have a valid reverse DNS look up for your mail server. Doing a search through http://www.dnsstuff.com and obtaining a DNS report for your domain can aid you with these issues. Many networks drop mail if there is no reverse DNS lookup for an IP address, or if the domain in the EHELO/HELO records are flawed.

Are your message headers clean and correct? Same Spade publishes a nice utility, which you can download and use to check your headers and make sure all is ok. If not, you will have to look into re-configuring the server you are using to ensure the message headers are set up properly.

Reply to challenge responses; occasionally, SPAM filtering software will send back a reply to your email asking you to confirm that you are a real person. Invest the 30 seconds or so it takes to do this for each challenge response you receive. Not only will it ensure that this particular recipient receives your message, but it can improve your sender reputation as well.

Meitasoft Inc. All Rights Reserved 1/14/2010