



THE E-MAIL MARKETING HANDBOOK IV

e-mail deliverability: are we there yet?

A complimentary white paper from Accucast

www.accucast.com
877-4-ACCUCAST

The Delivery Dilemma

A recent client survey revealed over 92 percent of e-mail marketers are somewhat to very concerned with e-mail deliverability issues, underscoring the business value of an effective e-mail marketing tool. Of the nine topics referenced, respondents identified e-mail filters (92 percent) and/or ISP blocking (73 percent) as their top concerns.

Survey respondents identified their greatest e-mail marketing challenge as having their messages perceived as Spam, which may cause recipients to ignore or delete permission-based messages.¹

All these barriers against unwanted messages can wreak havoc on legitimate, permission-based e-mailers, and many of their messages may be ending up in the trash bin. Consider these astonishing realities:

- AOL claims to block more than 1.4 billion pieces of Spam each day.²
- 34 percent of marketers have not taken any steps to improve delivery.³
- Hotmail's rate of "false positive filtering" increased from 5.6 percent in 2Q '05 to 9.4 percent in the third quarter, and Gmail's from 4.1 percent to 7.17 percent⁴

As daunting as the data seems, there are ways to achieve accurate, timely, cost-effective message delivery. This information-packed handbook examines the forces that may be hindering your deliverability and outlines strategies to increase the likelihood of every legitimate e-mail reaching its intended destination.

E-mail Deliverability Hurdles

Understanding deliverability hurdles is the first step to overcoming them. Take a look at the key barriers and what they mean to you and your business.

¹ Source: Survey Socketware 8/30/2005

² Source: 1) <http://www.imediaconnection.com/news/6520.ESPH> 8/12/05

³ Source: Jupiter Research 6/28/2005

⁴ Source: http://www.marketingvox.com/archives/2005/10/11/hotmail_gmail_filter_out_more_permission_emails/index.php

Authentication

Definition: (au·then ti·ca tion *noun*) The verification of the identity of a person or process. In a communication system, authentication verifies that messages really came from their stated source, like the signature on a letter.

In recent years various companies have created authentication systems to help legitimate senders be recognized by the ISPs. There are two methods of authentication: IP-based and Cryptographic. While neither method is the cure all to your deliverability needs, by implementing both methods your delivery rates and your chances of being recognized by ISPs will increase.

- IP-Based—This approach ties a responsible sending domain back to a set of ISP maintained IP addresses that are permitted to send mail from the domain.
 - Examples: Sender Policy Framework (SPF) and Sender ID Framework (SIDF)
- Cryptographic—This approach uses a public key encryption to “sign” each message in a way that proves the message came from the purposed sending domain by verifying the DNS domain of the e-mail sender and the message integrity.
 - Examples: DomainKeys and DKIM
 - DKIM uses Domain Name System (DNS) in the same manner as DomainKeys. DKIM also leverages Identified Internet Mail's header-signing technology, ensuring signature consistency as messages are sent through the network.
 - There has been large industry cooperation in helping to create, test and standardize the specifications of DKIM including AOL, Yahoo!, Earthlink, MSN, Cisco, VeriSign and others.

While only 17 percent of marketers have implemented sender identity records (e.g., Sender ID)¹, more companies are implementing this and other methods, including Domain Keys, everyday. As these authentication methods continue to gain adoption by senders and become more important to ISPs, there are some who continue to rely on the tedious process of whitelisting at specific ISPs.

Blacklists

Blacklists are published lists of mail servers and addresses known to be sources of Spam. Created and maintained by independent organizations, they are used by ISPs and bandwidth providers to filter out Spam sent across their networks or to their subscribers.

Each blacklist has its own policies determining what sites/IP addresses should be listed and although the goal is to filter out undesirable traffic, they can sometimes block legitimate senders. Among the reasons legitimate servers are blacklisted are:

- Problems with the sender's server settings that might allow unauthorized e-mail to be sent by individuals other than the server's owner.

- The IP address may be within a range of addresses the blacklist maintainer considers a source of unwanted e-mail, such as an ESP that, currently or in the past, has hosted questionable senders.
- An IP address may have been recycled from one previously used by a questionable sender.
- A complaint has been filed with a blacklist about the company.

Spam Filters

Spam filters are software programs that scrutinize the contents of incoming e-mail messages for keywords and other indicators identifying them as potential Spam and apply a scoring system to each rule. Once detected, and a score is applied, messages are either sent to the inbox, a junk mail folder or directly to the deleted items folder. This depends on the score it received and how much importance the ISPs put into the Spam filtering software.

The wild proliferation of Spam is forcing many ISPs to filter more aggressively—sometimes leading to false positives, or unintended censoring of legitimate e-mail. One way to avoid having your messages being blocked from Spam filters is to use a message scoring system, such as Accucast's Filter Advisor before you send the message to your recipients.

Bounces

By understanding the over 20 bounce codes that ISPs might send back to the sender, you are better able to ensure future delivery of e-mails. Taking action on certain hard bounce codes will not only keep your database clean, but it will also ensure that you are compliant with various ISP rules. Dirty data that generates repeated bounces not only places an unnecessary burden on systems, it can also raise ISP suspicions which will force your e-mails to go through stricter filtering systems.

Anti-Spam Legislation

On Dec. 16, 2003, President Bush signed into law the Controlling the Assault of Non-Solicited Pornography and Marketing Act, also known as CAN-SPAM. The law requires e-mail marketers to include legitimate return addresses and opt-out information in all e-mail messages they send.

While the law is intended to outlaw the techniques used by many Spammers, respectable companies need to ensure that they are compliant with the laws at all times. As this is a law that continually changes, with updated definitions and additions to the law, all senders should continue to follow the law or work with a provider that issues updates whenever needed.

ISP Rules

The ISP's job is to deliver wanted e-mail, while getting rid of the unsolicited variety that costs them money and irritates their customers. To stay ahead of Spammers, protect legitimate e-mailers and keep up with the dizzying pace of electronic marketing, they must continually update their rules to help fight against Spam. By building relationships with the various ISPs

or using a service through your E-mail Service Provider you are better equipped to handle any new rules that may come about.

HTML Readability

HTML offers the highest e-mail response rates and is the best way to solidify brand awareness. However, different e-mail clients often render HTML differently, so even after proper formatting and testing, the same HTML e-mail can end up looking different to recipients. Individual standards are constantly changing, adding even more fuel to e-mail marketers' frustration. By using a content analyzing tool to test your templates before you send them to your database of customers you will be able to see exactly how the message renders in each e-mail client, as well as which e-mail clients suppress your images by default.

Now for the Good News

In spite of the obstacles, e-mail remains one of the fastest and most cost-effective marketing tools available. The challenge is keeping up with the technology, expertise and business practices being developed to take advantage of this unique medium.

Outlined below are the key action steps every e-mail marketer should take to ensure maximum deliverability and results.

Implement Authentication methods

Make sure that you, as the sender, are publishing SPF records. If you are using an ESP, make sure they are publishing their SPF records. Once the records are in place and published, the implementation of Domain Keys is important.

Adjust for Spam Filter Rules

It is possible for permission marketers to pass through Spam filters by understanding how they work and adjusting accordingly. Ground rules include: scoring e-mail campaigns against Spam filtering rules before sending them; proactively seeking good relationships with ISPs in order to better understand their requirements; carefully monitoring campaign results to detect problems; and ensuring lists are based on recipients who have opted-in.

ISPs at the Gate: Road Runner Gets Tough

ISPs are the gatekeepers to e-mail message delivery and they all have different rules and requirements. Among the toughest is Road Runner, whose strict Spam blocking tools include national and local block lists and a comprehensive inbound sending policy.

To ensure their subscribers receive e-mail they have legitimately requested, Road Runner subscribes to multiple services listing senders who have certified, via some pre-defined mechanism, that all mail they send is confirmed as having been requested.

Get Whitelisted

There are two parts to getting whitelisted for each sender—ISP whitelisting and personal address book whitelisting. The first involves working with ISPs to get on their list. By achieving this “whitelisted” status the sender will have to go through less filtering systems than non-whitelisted companies.

Personal address book whitelisting has to do with getting your customers to add your e-mail address to the list of contacts, this is the only way to ensure delivery of an e-mail to an inbox by an ISP. To achieve both of these forms of whitelisting you should:

- Know each ISP's whitelisting policies, rules and processes for getting approved to be on their list.
- Put whitelisting directions on your Web site sign-up forms and all e-mails, explaining to subscribers the importance of adding your address to their contact lists or address books.

Know When You're Blacklisted

You will not necessarily receive bounce messages when you've been blacklisted, even though your e-mail has not been delivered. Regularly check the major Spam databases and blacklists like MAPS, Spamhaus and SpamCop to ensure you, or your e-mail provider, have not been added. If you have been added to a blacklist what should you do next?

- › First determine the overall impact of being on the blacklist?
 - › What is the adoption of the blacklist? (Which domains use the blacklist?)
 - › Look at your domain breakdown.
 - › What percentage of delivery do I think is being sacrificed?
 - › Consider the resources required for removal - If the percentage is low, consider not doing it. Most blacklists cycle names and IP addresses off over time.
- › If you determine that you want to get removed from the blacklist
 - › Go to removal links on the blacklist's Web site (most have them)
 - › Remember, blacklists are operated by individuals and independent organizations. Many do not have a way to contact them directly—no matter how legitimate your company or your complaint

Know Your E-mail Service Provider

A good e-mail service provider can be an invaluable ally in the quest for deliverability. Conversely, one who is in the business of simply sending e-mails, whether it goes into the inbox or the Spam folder, could potentially be a liability. Before choosing a provider, know:

- The nature of their relationships with the ISPs.
- How they identify and resolve ISP conflicts.
- What other clients they serve.
- What their UCE policies are.
- Whether or not they're whitelisted with major ISPs.
- How they handle AOL Spam complaints.
- What tools they use to test for Spam filtering.

- How they monitor campaign activity.
- How they verify HTML readability.
- How they respond to blacklisting.

For more details on evaluating a service provider, see Appendix A of this article.

Take Advantage of Deliverability Services

Even the most savvy industry experts admit e-mail marketing is becoming increasingly complex and sometimes downright confusing. Staying abreast of ever-changing rules, developing legislation and emerging trends call for marketers to take an active role in keeping their companies on the forefront.

Fortunately, the need for more sophisticated solutions has spawned a new breed of service providers who are adept at reducing Spam complaints and blacklisting, predicting and correcting HTML readability problems, and eliminating unnecessary ISP filtering. Many of these firms have excellent relationships with the ISPs, and can leverage their inside perspectives to improve deliverability for their clients.

Manage Bounces

Actively managing bounces can reduce costs, increase transactions and boost e-mail ROI. Use these proven tactics for driving down your bounce ratio:

- Clean your lists. Check for incorrectly formatted addresses, invalid domains and typographical errors.
- Pre-test your e-mails before sending to your entire list by sending a test to yourself and others. Be sure to include all the major e-mail services used by your recipients.
- Prompt customers to update information when they're making transactions.
- Set and adhere to a bounce threshold, or the number of bounces that must occur in a given period before an e-mail address is purged.
- Follow rules set up by ISPs for which SMTP bounce codes indicate an immediate need for address removal
- Include subscription/account management links in e-mails for easy updating of e-mail addresses.
- Monitor delivery rates by domain. If one is significantly different or you experience a sudden change, you may have a filtering or blacklist problem.
- Remove "Spam flag" addresses that can be added to your list maliciously. Examples are abuse@somedomain.com, postmaster@somedomain.com and noSpam@antiSpam.net.

- Confirm e-mail addresses by sending an auto-reply confirmation when a user subscribes, registers or makes a purchase. If that message bounces, attempt to correct it right from the start.

Keep Up with Legislation and Trends

Although the CAN-SPAM Act of 2003 is considered by many to be a step in the right direction, it's certainly not a cure-all. Loopholes, broad interpretations and weak enforceability are already being exploited, and some see even stricter policing on the horizon. Knowing where legislation is headed and what changes may be necessary to comply with both U.S. and international e-mail laws will be more critical than ever.

Leverage Your Provider's ISP Relationships

Any good e-mail service provider has long-established relationships with the ISPs and can navigate the processes more effectively than most marketers can on their own. By leveraging these powerful relationships, you'll be more likely to be alerted to deliverability issues before they become problems. If you do run into problems, the use of these experts will drastically reduce the time spent fixing them so that future mailings will not be effected.

Continually Monitor Campaign Activity

Monitoring of campaign activity is critical to identifying and resolving deliverability issues, bounces and ISP conflicts.

Keep Lists Up to Date

As mentioned earlier, dirty data can raise unwarranted suspicions from ISPs. Delete addresses that bounce after a set number of attempts, be cautious about renting lists and always remove subscribers' names immediately on request.

Confirm Readability

All HTML e-mail should be checked against multiple e-mail clients to make sure it looks the way you intended when it arrives. Some e-mail service providers have tools that can check the content before it's sent, and make recommendations on tweaking it for maximum visibility and consistency.

It's All Worth the Effort

Jupiter Research estimates annual e-mail marketing campaign expenditures will grow from \$1.4 billion in 2004 to \$8.3 billion in 2007.⁵ Smart companies recognize the power and potential of the medium, and they're investing the resources needed to ensure they get their share.

The deliverability "to-do" list is long, but achievable. An awareness of the factors impacting e-mail marketing today and a commitment to proactively manage them are clearly the keys to success.

⁵ Source: Jupiter Research, 1/28/04

Deliverability Quick Tips

1. Remove Spam Trap addresses from all sources—people add e-mail address with the word Spam in there
2. If you don't already published your SPF records—start
3. Begin preparing to implement DomainKeys and DKIM
4. Implement deliverability monitoring tools
5. Remove bad addresses from your list after a set number of bounces.
6. Send regular e-mails to remind recipients of your company and reduce Spam complaints.
7. Ask subscribers to add you to their personal address books
8. Stay updated on e-mail filters and mail delivery factors, or ask your e-mail provider for help.
9. Establish relationships with ISPs (or leverage your e-mail provider's relationships) to keep up with the latest rules and deliverability issues.
10. Monitor blacklists to ensure you aren't erroneously placed on one.
11. Stay abreast of e-mail marketing legislation and industry trends to be sure you comply with the latest developments.
12. Format HTML e-mails to avoid errors that could brand you as a Spammer.

Deliverability Dictionary

Address recognition: Occurs when a recipient puts a sender's e-mail address in an address book or a local whitelist that keeps e-mails out of the bulk mail folder.

Blacklist: A published list of IP addresses known to be senders of Spam.

Blocking: Occurs when a receiving e-mail server prevents an inbound message from reaching an inbox.

Bonded senders: Organizations that, for a fee, certify an e-mail sender as a "good guy" who conforms to permission marketing standards.

Bounced e-mail: E-mail that is returned to the sending server because of a non-existent address, a full mailbox or an unavailable server.

Challenge Response: When a recipient marks a sender as someone they want to receive mail from.

Confirmed opt-in: When a user elects to receive e-mail newsletters or standalone commercial messages. A confirmation e-mail is sent to the user, who is not required to take further action to be included on the list.

Double opt-in: When a user elects to receive e-mail newsletters or standalone commercial messages. A confirmation e-mail is sent, and the new subscriber must reply before he/she can be added to the list.

False positive: Occurs when a legitimate permission-based e-mail is incorrectly filtered or blocked as Spam.

Filter: Software used to block e-mail based on content in the "from" line, "subject" line or body copy.

Readability: An e-mail client's correct rendering of HTML e-mail.

Volume blocking: Occurs when a mailing containing a large number of obsolete or bouncing e-mail addresses reaches the ISP's bounce threshold and causes the rest of the mailing to be junked.

Whitelist: The opposite of a blacklist. ISPs create whitelists of e-mail senders approved for delivery despite blocking measures.

Appendix A

The Truth About Deliverability: Top Five Questions to Ask Your Service Provider

- **Are you whitelisted?** If the service provider is whitelisted, an ISP recognizes them as a legitimate e-mail marketer and your e-mail has a much better chance of being delivered. With a number of ISPs, whitelisting is not the end of the line because policies and processes to make it happen are not well-defined. Not all ISPs offer whitelisting and not every service provider will be whitelisted with every ISP. Only active, flexible relationships with key ISP contacts can ensure your mail gets through.
- **What's the nature of your relationships with ISPs?** If your current or prospective e-mail marketing provider claims to have relationships with ISPs, understand that these relationships are fluid and often undefined. It's important to know these relationships are not the magic bullet to solving deliverability issues. Navigating the relationships and processes inside these companies to get problems resolved can be challenging, so industry experience is critical.
- **What authentication methods have you implemented?** By understanding what methods your e-mail service provider has implemented, whether you use them as an ESP or purchase software from them, you will know that you will have a qualified resource to help you with the implementation of these systems
- **Do you have clients that send questionable content?** If you're using or considering a hosted e-mail marketing solution (ESP), and if other clients using the same provider send questionable content, your deliverability could be affected. Ask certain key questions like: Do you have a policy against Unsolicited Commercial E-mail (UCE)? How often do you bend that rule? Have you ever shut down a client? Make sure your e-mail provider continually monitors campaigns at setup and beyond to ensure clients are not exposing themselves and others to the risks associated with questionable content.
- **How do I know my e-mail will get through the spam filters and that my HTML will look okay in different e-mail programs?** Many e-mail providers believe they are in the business of sending e-mail, not getting it delivered. Whether you are considering an ESP or an in-house software solution, you need integrated tools that provide a high level of certainty your e-mail will get delivered, and your HTML will look great when it gets there. Make sure that your provider has tools that allow you to test your e-mails before you send them out to your customer base.

E-mail service providers should be able to address these questions honestly and openly with you. Remember, you shouldn't settle for anything less than a provider that can both guide and support your e-mail communications strategy.