

October, 2002

www.assurancesys.com

An Assurance Systems Brief: **Avoid the Spam Filter Trap**

Executive Summary

A minimum of 12% of permissioned e-mail messages is not properly delivered because they were incorrectly identified as spam.

The lost revenue for a marketer with a one million-address list could exceed \$1.4 million per year

Seven common-sense steps can dramatically reduce the size of the problem

Email is a quickly becoming the essential customer contact tool for both Business-to-Business (B2B) and Business-to-Consumer (B2C) marketers. Direct marketers spend massive resources making sure that their e-mail messaging drives optimal results. Unfortunately, at least 12 percent of permissioned e-mail messages do not arrive in the inbox as intended because the receiving ISP incorrectly identifies those messages as spam.

These "false positives" present a large problem for e-mail marketers, including:

- Lost Revenue
- Inaccurate Campaign Measurement
- Monitoring and Mitigation Costs
- Diminished Reputation

For a marketer with a list of one million addresses, the lost revenue could exceed \$1.4 million per year.

There are seven common-sense techniques that an e-mail marketer can follow to avoid being incorrectly tagged as spam:

1. Reduce the unnecessary volume demands on the receiving ISP
2. Follow permission best practices
3. Choose the ISP to host your e-mail server carefully and/or choose your e-mail service bureau carefully
4. Minimize the use of "spammy" keywords in the subject, from line and message body
5. Properly configure e-mail delivery infrastructure
6. Monitor continuously
7. Develop good relationships with ISPs

This white paper details the steps that an e-mail marketer can take to minimize the chances of campaigns being incorrectly identified as spam.

About Assurance Systems

Assurance Systems is the leader in developing tools and services to ensure that permissioned e-mail campaigns make it to recipients as intended. Please visit us at www.assurancesys.com.



www.assurancesys.com

E-mail is Customer Contact “Killer App”

Email is a quickly becoming the essential customer contact tool for both Business-to-Business (B2B) and Business-to-Consumer (B2C) marketers. According to eMarketer, the number of solicited commercial marketing messages that will be sent is expected to grow from just under 20 billion messages in 2000 to more than 100 billion messages by 2005. Within the last five years, e-mail has become an almost ubiquitous tool (see “E-mail: Everyone’s Doing It”)

E-mail has now expanded to include mission critical applications such as:

- Bill presentment
- Statement presentment (financial statements, frequent flyer statements, etc.)
- Shipment notification
- Transaction notification

E-mail: Everyone’s Doing It

- 75% of businesses have e-mail lists
- 15% of interactive sales come from e-mail promotions
- 13% of total marketing budget is spent on e-mail (fastest growing channel)

Source: Assoc. for Interactive Marketing

Direct marketers spend extensive resources making sure that their e-mail messaging drives optimal results. They optimize the individual elements of each message and campaign (list, creative, copy, hard offer, HTML vs. Text, etc.). Unfortunately, once the messages are sent, the marketer loses control of the process.

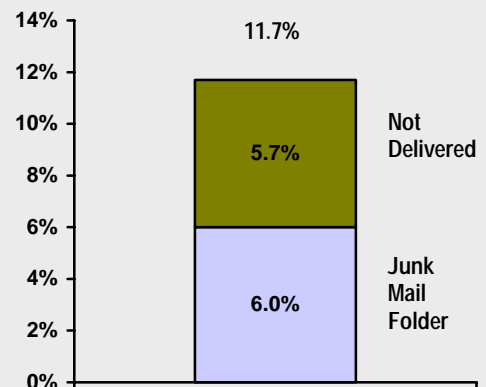
Your E-mail Messages Aren’t Getting There ... And You Don’t Know It

A recent study by Assurance Systems indicates that approximately 12 percent of all e-mail messages sent to valid e-mail addresses at the top nine ISPs and webmail providers did not end up in the inbox as intended. Rather, the e-mail either ended in the bulk/junk mail filter or was not delivered at all.

There are two primary causes of non-delivery to a valid e-mail address for bulk marketing messages are:

- **Transient Technical Problems** – Occasionally, ISPs will suffer temporary technical problems that prevent them from being able to deliver to a valid e-mail address. This is most common during peak usage hours when the ISPs e-mail infrastructure is being overwhelmed by too many e-mail messages.
- **False Positives** – A good deal of the inbound message volume that ISPs receive is unsolicited commercial e-mail (“spam”).

Non-Delivery of E-mail Messages



Source: Assurance Systems

ISPs estimate that up to 50 percent of message volume is spam. ISPs use a variety of techniques to combat spam that will occasionally flag a valid, opt-in message as spam.

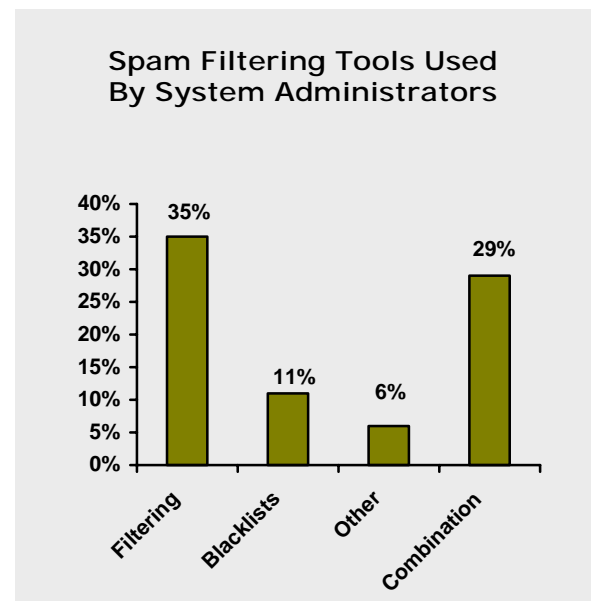
Because of the way that ISPs process mail receipt, the marketer doesn't always know the actual delivery status for a message. For example, when e-mail messages are diverted to the junk or bulk-mail folder, no bounce message is sent to the marketer indicating that the message did not make it into the inbox. In addition, some ISPs will "accept" delivery of all messages and process delivery on the back end. When the ISP's anti-spam filter comes across a message that looks like spam, no bounce message will be generated.

Your Messages Are Being Treated as Spam (The "False Positive" Problem)

The tools that the ISPs use to handle this unprecedented volume of spam are imperfect. Although each will filter out spam, they will often filter out legitimate opt-in e-mail. The most commonly used tools are as follows:

- **Content-based Filters –**

Messages can be treated as spam because they share some of the characteristics of spam. Content-based filters block messages that have content that "look like" spam. This software searches the body, subject, sender (as well as the rest of the message header information) for keywords and other indicators that identify the message as potential spam. Overly broad filters will cause legitimate messages to be tagged as spam. For example, content-based filters often use commonly used phrases such as "valued customer" and "click below" as an indicator that the message may be spam. In the Assurance Systems deliverability study, **more than 30 percent of messages were tagged as spam by one of the most commonly used content-based filters.**



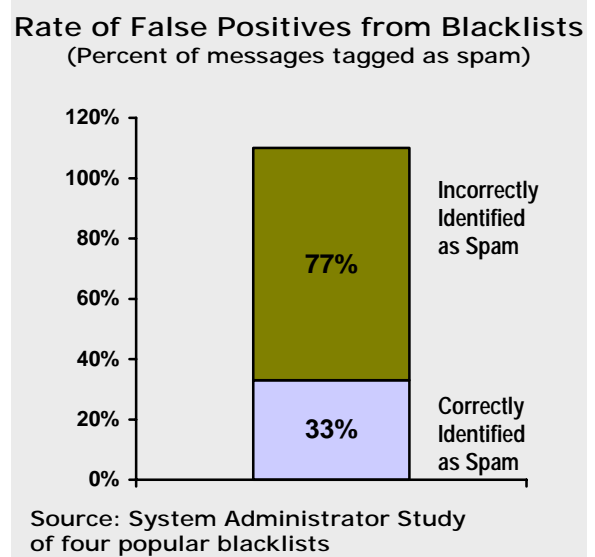
Source: eWeek

- **Blacklists –** The marketer's outbound mail server may reside on a "blacklist" of spammer-related IP addresses. A blacklist is simply a list of IP addresses that are associated with spammers. Receiving mail servers use these lists to determine whether to permit delivery of mail from the sender. Mail Abuse Preventions System, LLC ("MAPS") compiles the most well known blacklists. However, ISPs and System Administrators use more than 300 blacklists. Since many blacklists are developed by System Administrators to block bulk mail senders that they personally find troublesome, the definition of "spammer" differs by list. Often IP addresses of ISP that hosts an alleged

spammer are listed (rather than just the supposed spammer's IP block). A legitimate opt-in marketer can easily find himself on a blacklist. In the Assurance System's deliverability study, **100 percent of all permission-based marketers studied were on at least one black list.**

How can this be? Two reasons:

1. First, the definition of spam is far from universal. For some of these lists, only the strictest opt-in and unsubscribe procedures are sufficient to stay off the lists. Moreover, on most blacklists the marketer is presumptively guilty ("you are guilty until proven innocent"). This is not to say that blacklists do not list actual spammers. They do.
2. Blacklists will often punish ISPs for hosting those they define as spammers. This is an effective way to get the ISPs attention, but has the unfortunate side effect of blocking legitimate marketers that happened to be using that particular ISP. In a recent study by a Canadian system administrator, approximately **75 percent of the messages that were tagged as spam by four popular blacklists were actually legitimate, opt-in marketing messages.**



- **Volume-based Filters** –Messages may be blocked or redirected to the "junk mail" filter if the sending mail server exceeds certain volume thresholds. The volume-based threshold may be defined as bandwidth, messages per second and/or number of simultaneous connections from a given server. The volume-based thresholds differ between ISPs and are not public knowledge. Volume-based filters have nothing to do with a particular message being spam. Rather, it is a way for an ISP to protect itself from high volume demand.

The Impact of the False Positive Problem

The impact of having one in eight marketing messages (sent to valid addresses) fail to arrive in the inbox as intended is large. The impacts fall into four categories:

- **Lost Revenue** - For a list of one million active addresses the annual cost of the false positive problem can approach \$1.4 million per year (see *"Revenue Impact of False Positives"*).
- **Reputational Impacts** – Customers will miss expected communications. A missed bill, account statement or newsletter will diminish the marketer's goodwill with the customer.

Revenue Impact of False Positives

$$\begin{aligned}
 & 1 \text{ million-record list} \\
 & \times \text{ 12\% non-delivery rate} \\
 & = 120,000 \text{ not delivered} \\
 \\
 & \times \text{ 8\% Click-through rate} \\
 & \times \text{ 4\% Conversion Rate} \\
 \\
 & = 384 \text{ lost sales (@\$100 per sale)} \\
 & = \$38,400 \\
 \\
 & \times \text{ 36 mailings per year} \\
 \\
 & = \text{\$1.4 million}
 \end{aligned}$$

- **Increased Monitoring and Mitigation Costs** – Many marketers monitor a set of e-mail accounts across the most popular ISPs to determine delivery status of campaigns. This requires a significant number of man-hours as well as the cost of the ISP subscriptions. **To properly monitor the top 15 ISPs and webmail providers would require approximately 150 e-mail addresses that would cost in excess of \$400 per month for the ISP charges alone.** In addition, if problems are found the marketer has to contact the ISP and/or blacklist to resolve the problem, which takes additional effort.
- **Inaccurate Campaign Metrics** – As indicated earlier, the way that ISPs process "spam" mail receipt, the marketer doesn't always know the actual delivery status for their campaign if the message is treated as spam. This results in an inflated "delivered" number for a campaign and makes performance (click-through rates, etc.) look low.

So What Can You Do About It?

The good news is that there are some tangible, tactical steps that a marketer can follow to minimize the false positive problem.

1. Reduce the Unnecessary Volume Demands on the ISPs. Excessive volume demands will put you in the bulk mail folder (or get you bounced altogether). In addition to keeping track of volume demands, ISPs will often keep track of whether a particular mailer is attempting to send an excessive amount of mail to invalid e-mail addresses. If a mailer sends to an excessive number of invalid accounts, they may be blocked.

Some basic steps will minimize volume demand on ISPs:

- **Remove Bounces** – If you do nothing else, do this. If you deliver your own e-mail, use the bounce processing capabilities that are built into your "delivery engine." If you use a service bureau, make sure that it is removing bounces.
- **Use an E-mail Change of Address Service** – Approximately 30 percent of your e-mail list will churn over the course of the year because your customers have changed their e-mail address (new job, new ISP, etc.). Utilize an e-mail

change of address service to find new, up-to-date addresses for your customers.

- **Explore List Hygiene** – More than one percent of a typical e-mail list contains e-mail addresses that are not deliverable because of clear typos (for example, jsmithaol.com should clearly be jsmith@aol.com). You should use automated list hygiene programs to achieve this cleanup. Return Path (www.returnpath.net) provides both E-mail Change of Address and automated list hygiene services.

2. Following the Permission Best Practices. Marketers and members of the anti-spam community often have a different definition of what constitutes appropriate permission standards. Therefore, be as conservative as your business will allow in your permission practices.

It's important to not be labeled a spammer, because: (1) you will show up on blacklists which will limit your ability to get your e-mail delivered, and (2) It will make it difficult in your conversations with receiving ISPs.

Based on a review of the newsgroups frequented by the anti-spam community, the following steps will minimize (though not eliminate) your chances of getting into trouble:

- **Use the Most Conservative Permission Standard That Your Business Will Support** – Most marketers use “confirmed opt-in”. That is, when an individual signs up to receive mailings from a marketer, they are sent a message to confirm that the user signed up for the e-mail (and often giving an unsubscribe link in that e-mail). The people that compile black lists do not see confirmed opt-in as being sufficient to protect an individual from being signed up by a third party for a list. The preferred method is to require that the recipient of the confirmation e-mail click on a link from the e-mail or reply to the e-mail to be put on the list. There is a tradeoff in setting permission levels. If you make the permission standard more conservative, you will have a smaller list that is more likely to make it to the inbox. Each business will need to make that tradeoff in the context of their e-mail marketing strategy.
- **Capture IP Address of Subscriber** - If you want to go for extra points, you might want to capture the IP address from which the end-user signed up to receive publications as well as the time. This is a useful tool to remind a subscriber that they actually did sign up for the mailing after all and makes conversations with ISPs and Blacklists a lot more fruitful
- **Rent Lists Carefully** – Thoroughly investigate the source of the lists that you are renting. Sign up for the list as a subscriber. Were you given notice and choice? Did you receive a confirmation notice? Did this list use verified opt-in? How many messages did you receive? Too many? Now unsubscribe to the list. Does the unsubscribe function work? You can use a trustworthy list broker to help you determine which are the quality lists.
- **Make Unsubscribing Easy** – Have an easy to find unsubscribe link in every message and on your website. Make the process a 1-2 click experience for the subscriber.
- **Remove “Spam flag” Addresses** - Remove addresses from your list that may have been maliciously added to you list. Examples are: abuse@somedomain.com, postmaster@somedomain.com and nospam@antispam.net.

3. If You Are Delivering Your Own Campaigns, Choose the ISP that Hosts Your Mail Server Carefully. If You Are Outsourcing Delivery, Choose your Service Bureau Carefully. These partners will determine a lot of the success and failure you will have in making sure that your campaigns get through. As indicated above, an ISP may be blacklisted (or a large part of its IP range) for hosting a purported spammer. The same is true for service bureaus. If you review the newsgroups and discussion lists where spam issues are discussed, you can get a good idea if your service bureau or ISP is considered reputable. Review the NANAE (news.admin.net-abuse.email) newsgroup, the NANAS (news.admin.net-abuse.sightings) newsgroup.

These are available and searchable on Google Groups. In addition, sign up for the Spam-L discussion list (<http://peach.ease.lsoft.com/archives/spam-l.html>). The archives of the list are searchable. Search for the name of your ISP or service bureau across these lists to see if they appear to have a problem. It's worth noting that everyone gets at least a few mentions. However, if there are hundreds of entries about a given service bureau or ISP, there may be a problem.

4. Minimize the Use of Keywords in the Subject, From and Message Body That Might Look Like Spam to a Content-based Spam Filter. There are thousands of rules that are used. The follow rules appear to most commonly trip up marketers:

- "Free" (This is the kiss of death)
- The use of CAPS in the Subject line
- The excessive use of \$\$, !!! or other punctuation marks
- Excessive use of "click here"
- Redundant unsubscribe instructions and/or explanation of why user is on the list.

This use of a few of these keywords will probably not immediately mark you as spam. Be judicious in your use.

Assurance Systems provides a service, Message Checker, that the minimizes the chance of your messages being identified as spam before you send the campaign by checking your messages across hundreds of commonly used spam-filtering rules and identifying rules you have violated.

5. Properly Configure E-mail Infrastructure. The improper configuration of the technical infrastructure that supports e-mail delivery may make your campaigns appear to be "spammy" to ISPs. The following steps will minimize the most common problems:

- **Enable Reverse DNS Lookup** – Many e-mail filtering packages will use reverse DNS lookup to make sure that the company that is supposed to be sending the message is actually the company sending the message. If reverse DNS is not enabled, then your mail may not get through.

- **Check for Open Relays and Close Them** - If your e-mail server allows other e-mail servers (outside your control) to relay messages through it then it is has an "open relay." Spammers most often use open relays to send their messages. Many blacklists consist of known open relays. If you have an open relay, there is a good chance you will end up on one of these blacklists.
- **Don't Relay Between Servers Before Sending Out Messages** – Some e-mail marketers relay messages between servers within their control (usually in the same domain) before sending them on to the final destination. Making lots of hops between servers is one way that spammers cover their tracks. The more hops you make, the more you look like a spammer to filtering software.
- **Use a Secure Version of FormMail on Your Website (if you use it)** – FormMail is a commonly used script that allows mail to be sent from a form on a website. Security bugs in earlier versions of FormMail allow it to be hijacked by spammers to send messages from your mail server.

6. Monitor Continuously to See if You Have a Problem. There are a variety of ways to monitor whether you have delivery problem:

- **Monitor Delivery Rates by domain** - Track your delivery rates over time by domain. This data should be available from your service bureau or e-mail delivery software. For example, if you find a sudden drop in delivery rates at AOL, it may be indicative of a problem there.
- **Monitor Test Accounts** - The top 15 ISPs will represent ~60 percent of a typical B2C list. You should check each test account to see whether or not the campaign made it through to each test account or was blocked (or simply shunted to the junk mail folder.) To really do the job right, you will need to more than ten addresses across each ISP so that you can be reasonably sure that you can test the beginning, middle and end of your campaign. Assurance Systems' Message Checker service allows you to know when your campaigns are not getting through at major ISPs automatically (without having to manually check hundreds of accounts).
- **Monitor blacklists** - Check blacklists to determine if your mail server is on any prior to each campaign. If you use "triggered" e-mails (for example, a shipment confirmation) you should check that IP address daily. Assurance Systems provides a service, Blacklist Alert, which will alert you if your mail server's IP address is found in over 300 blacklists.

7. Develop Good Relationships with ISPs. You need to know who to contact when you have a problem. You will need to develop time and resources to developing a strong relationship. If you don't have the resources, consider using a service bureau that provides this sort of support and/or hiring an outside consultant.

###

About Assurance Systems

Assurance System provides tools to assure that your e-mail campaign makes it to the inbox as intended. Our tools include:

- **Message Checker** –Minimize the chance of your messages being identified as spam before you send the campaign. Simply send a test e-mail to Assurance Systems and Message Checker immediately tells you which elements of your e-mail are most likely to identify your message as spam to the most commonly used spam filters.
- **Delivery Monitor**– Now you can know when your campaigns are not getting through at major ISPs. If your messages are blocked by ISPs because they look like spam or end up in the junk mail folder, your e-mail delivery system has no way of telling you that the mail didn't get through. All you have to do is log into your personalized reporting page to see the delivery status of your campaign.
- **Blacklist Alert** – Be alerted when your mail server has been placed on a blacklist. The Blacklist Alert sends you a message if your mail server has been placed on one of more than 300 blacklists.

If you are interested in learning more about Assurance Systems, visit us on the web at www.assurancesys.com or contact our sales team at sales@assurancesys.com.

