



Global INTELLiSYSTEMS

Increase Email Message
Delivery
with Bounce Management
and Message Analysis

A Whitepaper By John Brogan
April 2007

Contents

Introduction	3
Section 1: Bounces Affect Reputation and Metrics	4
Section 2: Continually Ignoring Bounces Can Blacklist Mailers	5
Section 3: Action Without Enough Information Can Reduce Lists Unnecessarily	6
Section 4: Industry Lacks Bounce Standards	7
Sample hard bounce	7
Sample soft bounce	7
Sample filter or block bounce	8
Section 5: Spam Filters Use a Multi-Level Approach	9
Section 6: Reading and Interpreting Filter Bounces	10
Example 1	10
Example 2	10
Example 3	11
Section 7: Bounce Prevention Saves Time and Money	12
Section 8: Testing Just a Few Services Isn't Good Enough	13
Section 9: Select the Right ESP and Improve Your Deliverability	14
Global IntelliSystems, an ESP	15

Introduction

Many email marketers are not generally analyzing or even reviewing bounces following email campaigns. Most assume that bounces are just part of doing business. The “just send it again” mindset can quickly lead to a significant drop in delivery rates.

But the cost isn't only lost sales from that particular campaign.

Over time, ignoring the cause of bounces can not only result in damage to your general reputation but not addressing bounces can also adversely impact your ability to even perform email marketing.

1 Bounces Affect Reputation and Metrics

1

Bounces fall into two general categories: hard bounce and soft bounce.

Soft bounces are temporary failures. These occur because of technical difficulties such as servers being temporarily down or individual mailboxes are full.

Hard bounces are permanent failures. These messages are not deliverable due to incorrect or non-existent email addresses.

Email Experience Council (EEC) found that 66% of mailers don't have good visibility to their bounce metrics.

Mailers and Email Service Providers (ESPs) don't all define or treat hard bounces and soft bounces in exactly the same way. The definitions of a bounce matters because how a bounce is tracked can impact metrics such as deliverability and open rates. Not understanding how metrics are calculated can lead mailers to inaccurate conclusions and actions.

The recent Email Experience Council (EEC) survey report highlights the importance of bounce data and bounce management within email marketing. Mailers and ESPs both consider deliverability a very important factor. But, EEC found that 66% of mailers don't have good visibility to their bounce metrics. Perhaps even more of a concern is

that nearly 40% of ESPs can't isolate the specific reason for a bounce. In other words, they can't tell their clients which bounces are occurring due to bad addresses or which ones are bounced because of spam blocks or technical failures.

2 Continually Ignoring Bounces Can Blacklist Mailers

Spam filters are now complex yet very effective. Many ISPs consider preventing spam from reaching their customer's mail boxes a major commitment. The desire to block spam from reaching users results in tighter and ever-changing controls. The rulesets many anti-spam systems use often rely on third party databases and trigger words change on a daily basis.

ISPs monitor the number of bounces sent into their domains and the domains the bounces are sent from. ISPs often develop filters and blacklists as a result of the bounces they see. The issues mailers face if they don't review and take action regarding bounces can snowball quickly to the point that they can no longer deliver email to those ISPs effectively.

Filters can bounce messages for dozens of reasons with more than 350 different reason codes – there are more than 24 ways to say a mailbox is full these days.

This means that mailers need to always be vigilant and attentive to the results of their campaigns. Filters can bounce messages for dozens of reasons with more than 350 different reason codes – there are more than 24 ways to say a mailbox is full these days. Continuing to mail to domains that bounce your messages will get the ISP's attention and will cause a sharp decrease in inbox deliveries and a noticeable decrease in open rates because many ISPs will block or DOA mail from abusive mailers.

Mailers with too many bounce problems and/or mis-configured headers can be put on a blacklist. Even the suspicion of spamming can blacklist a mailer very quickly.

Hotmail, for example, has special "trap" mailboxes and keeps a close eye on bounces and deliveries associated with those addresses. If you mail to one of these trap addresses, it means you have a non-manicured list (lots of old addresses) or that you are accepting new subscribers

without using any confirmation process, (no confirmed opt-in). Hotmail watches your "trap hit rate." If it reaches a certain level, they will route your mail to the junk box and your inbox delivery rates will plummet.

Unfortunately, legitimate mailers can get caught in those same situations if they are not careful with their bounce management.

3 Action Without Enough Information Can Reduce Lists Unnecessarily

An in-house study by Global IntelliSystems over a three month period with 163 million sample deliveries showed that the bounce rate averaged 9.3%. Hard bounces – host or user unknown – accounted for 2.1%. Soft bounces – mailbox full or over quota – accounted for 5.4%. A mailer wanting to take action on those bounces, but not having any more data than the list of bounced addresses, could easily decide to remove all the bounces – eliminating good addresses unnecessarily.

The remaining 1.8% of bounces fell into the suspect bounce category, such as possible filtering or a non-standard bounce reply. These bounces pose the real problems for mailers because they are difficult to analyze. Most mailers simply ignore the hard-to-analyze bounces. Unfortunately, this group of bounces will only grow over time because many of them are spam filter bounces which, when unchecked, spread to other filters.

Many ISPs often bounce legitimate mail due to a spam filter, known as a “false positive”. But the bounce phrase makes the bounce appear to be attributable to “user-unknown.” Without proper bounce analysis software you may be removing legitimate email addresses from your list when the true cause was an overly aggressive spam filter. As you can see, bounces have a significant impact on your overall inbox success rate.

4 Industry Lacks Bounce Standards

One reason bounces are hard to analyze is that ISPs, corporate domains, and other email receivers provide inconsistent information in their bounce messages. This means that unless you are really tied into the industry, spend significant amounts of time reading bounce messages, and talk regularly to the people sending bounce messages you will frequently come up to a dead end and not know what sort of action is needed to resolve a problem.

Some bounces though are easy to understand. Here are a few examples of some of the more typical bounce text and recommended appropriate actions when these messages are received.

One reason bounces are hard to analyze is that ISPs, corporate domains, and other email receivers provide inconsistent information in their bounce messages.

Sample hard bounce:

```
----- Transcript of session follows -----
... while talking to aaa.bbb.ccc:
>>> RCPT To:<sample.user@aaa.bbb.ccc>
<<< 550 Message refused as "sample.user@aaa.bbb.ccc" is unknown
550 5.1.1 sample.user@aaa.bbb.ccc.. User unknown
```

Since the user is unknown, the right action is to delete the email from your list. If you continue to mail to these addresses, you run the risk of triggering a blacklist against your domain.

An additional action is to verify the bounce with the domain owner. If you received a sharp increase in bounces from the same domain, it may indicate that the domain has changed ownership and the list members did not notify the sender of the address change. Whenever a large number of bounces appear from the same domain, it is always best to take a moment and analyze the domain itself to determine if the cause is a simple change of address or something worse, a cloaked blacklist against you.

Sample soft bounce:

```
***** MAILBOX FULL *****
The mail has not been delivered to the recipient: sample.user@aaa.bbb.ccc
because that mailbox is full
Please try again at a later time
***** MAILBOX FULL *****
```

Industry Lacks Bounce Standards

In this case, you should keep the address on your mailing list and not consider removing it unless you continually get the same message. Always keep a running count on the number of times an address bounces for any reason. Many recipients may have a mailbox full status for weeks if they rarely check their email.

Sample filter or block bounce:

```
----- Transcript of session follows -----  
... while talking to aaa.bbb.ccc  
DATA  
550 5.7.2 This smells like Spam.  
554 5.0.0 Service unavailable
```

The message sent should be reviewed. For some reason, the ISP saw something that was suspect regarding the message. Was the text checked for spam triggers before it was sent? Is the header formatted properly? Are you using white text on a dark background? If the message appears clean, you need to look at the technical information associated with the message and determine if anything has changed that could be a flag for an ISP. If you can't determine the reason for being considered spam, contacting the ISP directly may be necessary.

5 Spam Filters Use a Multi-Level Approach

There are three levels that ISPs go through when making suspect spam decisions. So, to stay out of potential spam space, mailers need to consider the same three levels.

The first level is to examine the IP address and domain name of the sending server. To identify suspect spam, ISPs ask questions such as

- Is that server allowed to send mail (SPF/Sender ID Tests)?
- Is that server flagged as a “bad sender” (external blacklist)?
- Is that server on an internal blacklist or filter?
- Does that server have a working or valid reverse DNS setup for the IP address?
- Has that sender sent too much mail in the last 15 minutes?

The second level looks at the message header. Questions asked at this level include

- Is the message header properly formatted for this message?
- Are there any blacklisted domains or IP’s referenced in the header itself?
- Does the routing appear to be forged or irregular?
- Are there keywords in the header that match a filter rule?

The third level looks at the message itself asking questions such as

- Are there any URLs in the message that are blacklisted?
- Are the URLs improperly formatted?
- Are there any words or phrases commonly used in traditional spam?
- Does the message have any white or grey text on dark backgrounds?
- Is the message too heavy in HTML code vs. the text itself?
- Is the message using pure graphics and no actual text?
- Is it a HTML-only message vs. multipart?
- Do file names in images reference a blacklisted word or phrase?

There are three levels that ISPs go through when making suspect spam decisions.

6 Reading and Interpreting Filter Bounces

Some of the reasons messages get caught in spam filters can be gleaned from the bounce message. However, this is probably the least standard area related to bounce management. Here are a few examples and suggested cures.

Example 1:

```

... while talking to aaa.bbb.ccc.:
      DATA
554 5.7.1 Message rejected because of unacceptable content.
      For help, please quote incident ID 550120.
554 5.0.0 Service unavailable
  
```

This message was stopped during the DATA phase of the SMTP transaction. This generally indicates the message had words or phrases in the body that, when added up to a point value, pushed the message into the spam category. This is usually cured by reducing the number of trigger words commonly found in spam – free, act now, money, \$\$\$, ***, hurry – used in the message. Sometimes, common sense can cure these problems – ask yourself, “Would I consider this spam if I received it?”

Example 2:

```

----- Transcript of session follows -----
... while talking to aaa.bbb.ccc:
      DATA
554 5.7.1 mydomain.sender.abc [192.168.0.141]: Client host rejected:
      Access denied AS5101
554 5.0.0 Service unavailable
554 5.5.1 Error: no valid recipients
  
```

This type of bounce indicates the IP address or domain name is blocked by the sender. Likely, past bounce messages were not evaluated and handled and the recipient system now has set up a filter against you. The best cure for this is to have your ESP contact the domain holder to uncover the root cause of the blacklist and work with the domain holder to have the block removed.

Many ISPs will ask for evidence that the subscriber opted-in, then confirmed their subscription.

Almost every domain holder will remove a block if there are assurances by the sender that complaints and bounces are promptly dealt with if they come up. The sender also needs to assure and prove that a confirmed opt-in list is being used. Many ISPs will ask for evidence that the subscriber opted-in, then confirmed their subscription. If you don't have this data, you may be stuck on the blacklist until you change your list management practices.

Reading and Interpreting Filter Bounces

Example 3:

“Your mail to the following recipients could not be delivered because they are not accepting mail from aaa@bbb.ccc”:

This type of filter or block bounce is a classic AOL message. Yet, many mailers continue to mail to the same person again and again, in some cases for months. The recipient no longer wishes to hear from the sender. But instead of unsubscribing, they just add the sender to their blocklist.

The cure is to delete the user from your list. Changing your address often to slip past the filter and get through to these recipients only angers them. You are trying to reach them when they don't want to hear from you.

If you are sending a paid newsletter, contact the recipient directly and inform them of the bounce. They may have mistakenly marked your last message as spam.

7 Bounce Prevention Saves Time and Money

Scanning messages before they are sent may significantly help with your deliveries. Your ESP should have a set of tools that will evaluate your message in terms of how it ranks with major spam filters. Many mailers do not take this step and have a very high bounce rate due to filters. It takes only minutes to receive the results of a message analysis. Making subtle changes in the content can cut the number of spam bounces in half. Knowing what words and practices are being targeted allows you to address the issue before it costs you lost deliveries.

You should always have a 100% delivery rate to your seed mailboxes. If you get anything less you should not mail until you find and fix the root cause of the missed delivery.

“Seeds” are valid email addresses on many of the major ISPs and online services. Most ESPs have a few dozen email addresses you can use for your test mailing. After performing a scan on the content, you should send to those seed addresses to see how they appear when, or if, they arrive. You should always have a 100% delivery rate to your seed mailboxes. If you get anything less you should not mail until you find and fix the root cause of the missed delivery.

8

Testing Just a Few Services Isn't Good Enough

Global IntelliSystems conducted a survey of new clients coming onto the service and asked mailers how many seed addresses they used prior to their live launch. The results were amazing. Over 80% of the survey responders said they used only one or two test addresses. The assumption that “if they make it to two test mailboxes, they will make it to all” is dangerous and can be a significant reason for poor delivery and open rates. Always test with at least twenty addresses on almost all of the major ISPs and online services.

In addition to seeding ISPs and scanning your messages for spam triggers, many mailers are turning to accreditation or certification services. In this case, a third party records your email process and certifies that you are a legitimate mailer following guidelines and good practices. ISPs – particularly large ISPs such as AOL, EarthLink, Yahoo!, and Hotmail/MSN – check up on emailers. If a sender is certified as legitimate using one of these accreditation services, the emails are allowed to reach their destination, and almost always to the inbox. Companies providing accreditation or sender certification include Surety Mail, Habeas, GoodMail, and Sender Score Certified.

9 Select the Right ESP and Improve Your Deliverability

A knowledgeable and up-to-date ESP should be able to assist you with bounce management and provide reasonable assurance that you won't be classified as a spam source. Here are seven characteristics your ESP should possess.

1. The ESP will handle block clearing and filter issues directly with the domain holders or ISPs.
2. The ESP has seed boxes available for use on the major online services and ISPs.
3. The ESP offers to help analyze mailings for you prior to the live launch to help teach you how to “do it right.”
4. The ESP will provide a confirmed-opt-in (COI) system for you to use to ensure your list remains clean. They will also help you reconfirm your existing non-COI list.
5. The ESP will not just collect bounces for you, but will analyze the bounces into more than just hard/soft/blocks.
6. The ESP will help you uncover signs of blocks – and work to resolve them with the recipient system – after your first few mailings.
7. The ESP has extensive working relationships with the major ISPs and online services and will act as the liaison to ensure that current and future mailings are free-flowing with the ISPs and online services.

Do not assume that every ESP will have the time to provide the detailed services you need to conduct your professional campaigns.

Email marketing can be a major component of many businesses – but only if your messages reach your customers and prospects. Assuring that your emails are delivered and assisting with resolution of issues are signs of a good ESP. Analyzing your bounces and contacting ISPs to resolve issues are signs of a great ESP. Do not assume that every ESP will have the time to provide the detailed services you need to conduct your professional campaigns. Always ask the ESP detailed questions on how they will help you before, during, and after delivery – before you sign their contract.

Global IntelliSystems, an ESP

Global IntelliSystems, provides its customers with the most in-depth email marketing services available. Bounces are taken apart piece-by-piece and scanned for more than 800 phrases to identify even the most non-specific bounce. Working only with valid companies that do not engage in any spamming tactics, Global IntelliSystems assures that email is delivered and provides hands-on assistance to assure your campaigns are delivered every time. A good reputation makes all the difference with an ESP.

To find out how Global IntelliSystems can help you with bounce management and complete e-mail marketing services, visit <http://www.GLIQ.com> or call (800) 707-7074 today.