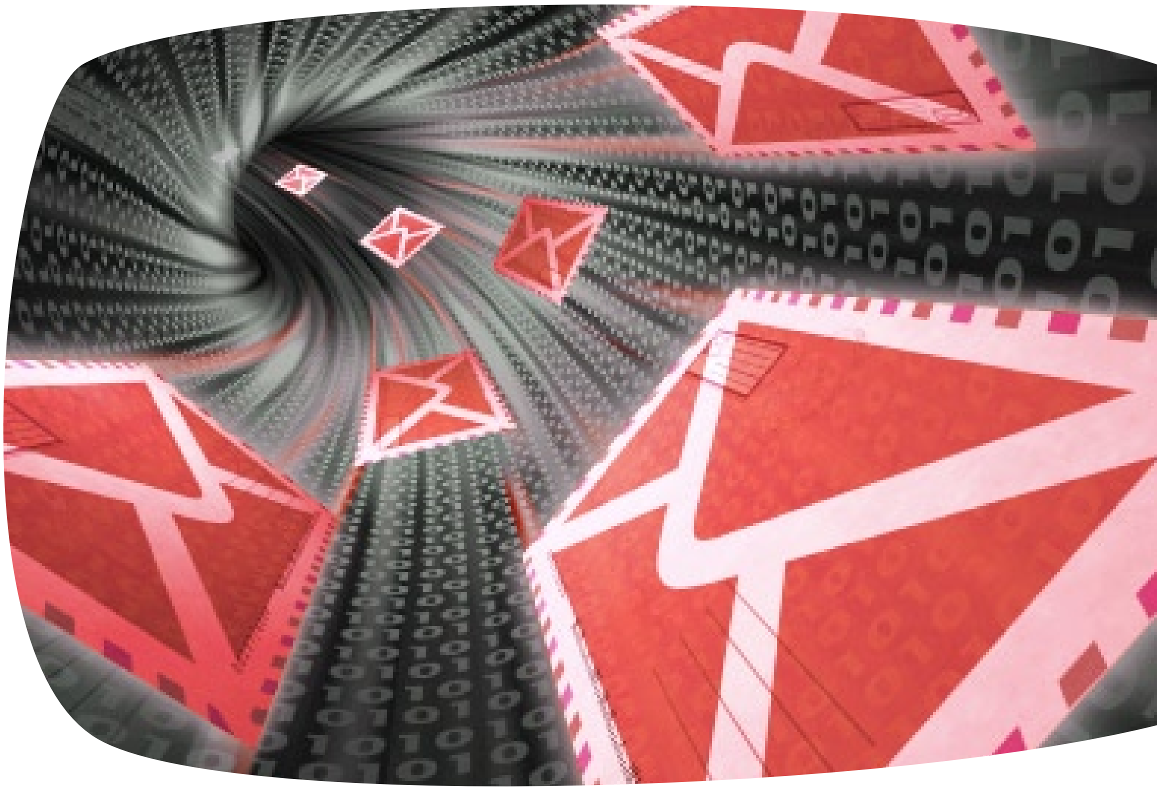
White Paper
Email Deliverability Review



Published by
Deliverability Hub of the
Email Marketing Council

Sponsored by

Contents

About this document

Email deliverability has become a formidably technical subject, and it would easy to write a formidably technical document on the subject. That was not our intention – there is plenty of detailed technical information available on the subject, and the "Further Reading" section will point you in the direction of some of those sources.

Rather, this document has been written for the email marketing programme owner who has realised that their broadcasts are starting to experience delivery problems, and are trying to identify why this may be the case. It highlights 10 of the major issues that affect email deliverability, and then provides common-sense guidance on how to deal with them.

About the authors

This document has been published by the Deliverability Hub of the Email Marketing Council of The Direct Marketing Association (UK) Ltd.

Published date:	January 2010	
First revised:	December 2011	
Written by:	Guy Hanson	Return Path
	Simon Bowker	eCircle
Edited by:	Jonathan Burston	CACI
	Skip Fidura	dotAgency
	Sara Watts	Data Media & Research
	Simon Hill	Extravision
Additional review by:	Tim Roe	Redeye
	Tim Watson	Zettasphere
	Richard Gibson	Return Path
	Matt Rausenberger	Return Path

Sponsor's perspective

With most major ISPs now implementing inbox placement prioritisation techniques, a new set of behavioural metrics are becoming increasingly important within the realm of email deliverability. The key messages to take back from this white paper are:

- The factors that influence email deliverability are starting to change. Instead of focusing their efforts on punishing 'bad' email, ISPs are now considering how to reward 'good' emails.
- This means that a new set of behavioural metrics are becoming increasingly important. These metrics are being measured through the use of engagement data to provide a view of whether subscribers are interacting positively or negatively with their emails, and this data is now starting to play an important role in determining the placement and positioning of these emails.
- Sender reputation remains the cornerstone of email deliverability, and the primary factors that influence reputation metrics (infrastructure, data quality, and complaints) represent the core factors that email marketers need to be monitoring. Now, however, the subscriber behaviours that are being observed are playing a rising role in determining the visibility that the senders' emails enjoy.
- The deliverability challenge has gone through a remarkable transition. Email marketers need to be aware that there are important new indicators for them to monitor in order to maintain a healthy set of deliverability metrics.

Guy Hanson,
Director, E-Marketing Response Consulting Services EMEA, Return Path
Chairman, Legal Data & Best Practice Hub, DMA Email Marketing Council

Executive summary

Over the past few years, the emphasis on email deliverability has changed substantially. Previously, the key question was a fairly simple one – "Why are my emails getting blocked, and what can I do to make sure that they don't?"

However, the current challenge is far more concentrated on achieving email delivery to subscribers' inboxes. Recent research by Return Path shows that average inbox placement rates currently stand at 76.5% globally, and at 84.5% for Europe[1]. In broad terms, one out of every five emails is not being delivered to the inbox.

Since the previous edition of this white paper was published, there has been something of a sea change in the way that ISPs and spam filter vendors have been dealing with unsolicited commercial email. The primary reason for this change in emphasis has been because of the massive volumes of spam that Internet Service Providers (ISPs) are attempting to deal with. According to the most recent McAfee Quarterly Threat Report[2], while there has been a recent reduction in global spam volumes, there are still approximately 1.5 trillion spam email messages being broadcast every day. The challenge for ISPs is to be able to identify (and eliminate) this volume without incurring collateral damage and preventing permissioned email activity.

Previously, the approach was to identify "bad" email, and block it. However, as spam volumes continued to grow exponentially, this meant that the number of false positives (good emails that were being incorrectly blocked) increased as well. The focus has therefore started to shift away from penalising "bad" email and toward rewarding "good" mail instead. This is being achieved through the use of engagement data to provide a view of whether subscribers are interacting positively or negatively with their marketing emails. This data is now starting to play an important role in determining the placement and positioning of these emails.

This revised document, therefore, has a brand new section that focuses on the challenges (and opportunities) that are posed by the increasing prevalence of smart inboxes. It has also fully refreshed the key factors that currently influence email deliverability, and the useful reading section has also been substantially extended. Readers are provided with an up-to-date understanding of the causes that may be compromising email deliverability, as well as 10 common-sense recommendations which, if adopted, will go a long way to ensuring that the sender's emails end up where they are going to be seen and actioned – in the inbox.

As with the previous edition, this is not intended to be a technical manual, and the 10 steps do not contain detailed instructions on how to implement each of the recommendations. However, in the final section ("Further Reading & Useful Links"), there are a number of references that readers can use to find out more about these key concepts, and how to go about achieving them. By implementing the recommendations outlined in this document, most e-marketers should be able to produce inbox delivery metrics that are at least broadly comparable, and often better, than the benchmarks quoted above.

[1] The Return Path Global Email Deliverability Benchmark Report, 2H 2011

[2] McAfee Threats Report: First Quarter 2011

1. Major factors that impact on deliverability

1.1 Sender reputation

In the not-too-distant past, the primary driver that determined whether ISPs would accept and deliver emails was the content of the email, and email marketers were very careful to ensure that their emails did not contain any of the trigger words that would cause them to run foul of these content-based filters.

More recently, however, this scenario has changed with the primary current consideration being that of sender reputation. This is something akin to a credit score for email broadcasters, and is informed by a range of factors, such as the volume of email that a sender broadcasts, the number of bounce-backs that they generate as a result of rejects and/or unknown users, and the number of spam complaint notifications that they receive.

In a recent study[3] by Return Path it was found that approximately 80% of email delivery problems are directly attributable to a poor sender reputation. It is therefore vital for email marketers to know what their reputation scores are, and to take remedial action if those scores are poor.

Sender reputation data can be used by ISPs in a variety of different ways:

- Whether to simply accept or reject email traffic.
- To determine what level of volume throttling (see section 2.4) to apply.
- In conjunction with other approaches such as spam filtering, authentication, etc.

It is easy to find out what score is currently being achieved by your email marketing activity (provided that you are generating sufficient levels of activity to register with the monitoring companies). Simply take the IP address that the email activity is being sent from, and use one of several publicly available websites (links at the end of this document) and run a lookup against that address.

Most of the sites will also provide useful information into some of the key metrics that are used to calculate the reputation scores. In this way, you can identify where your email programme is falling short, and take appropriate action to rectify those shortcomings.

It should also be mentioned that sender reputation is not necessarily IP address-specific. Increasingly, metrics are being managed at domain level, placing an onus on broadcasters to move away from operating "good" and "bad" IP addresses.

A key point is that responsibility for sender reputation rests with several different parties – marketers cannot abdicate responsibility for sender reputation to their technology partners, and the reverse holds equally true. While an ESP will be responsible for aspects such as infrastructure, bounce handling, and ISP relationship management, the marketer will control how the data is being collected, frequency of contact, quality of targeting, and so on. All of these factors affect sender reputation, and both parties have vital roles to fulfil in this regard.

1.2 Spam filtering

There are a variety of spam filter solutions in the market place, and they operate at a number of different levels:

- Desktop client filters
- Server filters
- Gateway filters

[3] See http://www.returnpath.net/landing/reputationfactors/

Some of the best known spam filter providers include:

- Barracuda
- BrightMail
- Cloudmark
- Commtouch
- IronPort
- McAfee
- MessageLabs (Now Symantec.Cloud)
- Postini
- Spam Assassin
- Vade Retro

These filters adopt a range of different approaches to the way that they process emails. Some of the most common approaches include:

- Bayesian Filtering: Particular words and sentences have particular probabilities of occurring in spam email and in legitimate email. These filters learn to predict emails to be spam based on the probability of appearance of different word combinations.
- Fingerprinting: This process calculates a checksum that uniquely identifies an email, for use in spotting duplicate messages. The checksum is based on: the Message-ID: header; the Date:, From:, To: and Cc: headers together; and the body of the message.
- Heuristic Filtering: Works by subjecting email messages through thousands of pre-defined rules against the message envelope, header and content. Each rule assigns a numerical score to the probability of the message being spam. The result of the final equation is known as the Spam Score.

In addition to B2C requirements, spam filter and anti-spam vendors tend to have two main B2B customer groups: ISPs, and businesses as end users. Deliverability is therefore just as much of a challenge in B2B as it is in B2C email marketing. However, the fact that ISPs such as Yahoo! and Gmail are host to many business domains means that the pre-deployment testing techniques that are employed for B2C email audiences are becoming increasingly relevant to B2B email audiences as well.

1.3 Blacklist operators

Blacklists contain records of e-marketing activity that has been identified as spam-like in nature. ISPs, spam filter vendors, and domain administrators will use this information as a guideline to determine whether they will process or reject incoming emails. Many spam filter vendors also operate their own individual blacklists.
The ways in which an email sender can become blacklisted take several different forms:

- RBL (Real-time Black List)
- DNSBL (Domain Name Server Black List)
- SURBL (Spam URL Real-time Blocklists)

In some cases, the email sender can be reported directly to the blacklist operator. Alternatively, the blacklist can be managed independently of consumer feedback, with the lists being populated on the basis of the operator's own observations and expertise.

Some of the better known blacklist operators include:

- Spamhaus
- Spamcop
- MAPS (Mail Abuse Prevention System)
- SORBS (Spam and Open Relay Blocking System)

There are a number of web-based tools which an email broadcaster can use to identify whether their email traffic is being blacklisted. Should blacklisting be identified, point 2.7 (Blacklists) of the next section provides some tips on how to get the listing lifted.

Broadcasters should be aware that these operators also make use of their own spam traps[4]. This places a premium in terms of ensuring that best practices are applied to the way that email addresses are sourced (see next section – "Improve Data Collection") so that email broadcasters do not get blocked as a result of broadcasting to spam trap addresses.

1.4 Smart Inboxes

Recently the impact of Sender Reputation upon email delivery has been increased further through the launch of new 'Smart Inbox' features. Gmail's 'Priority Inbox', which measures how users interact with emails from different senders, and decides whether or not those emails should be considered as priority, is the most notable example. Typically, emails from friends and colleagues are flagged as priority emails, and appear at the top of the inbox.

However, other ISPs such as Hotmail, Yahoo! and AOL have all followed suit, with inbox placement/prioritisation techniques that reward known sender status and/or positive engagement behaviour. For several years, Hotmail users could manually select the messages that are important to them, and relevant content would therefore be prioritised. In the case of Yahoo!, integration with Yahoo! messenger meant that all other emails are ranked secondary to those received from Yahoo! messenger contacts.

Hotmail has further raised the bar by targeting Graymail (or "bacn" – one step up from spam!). Graymail is represented by email such as newsletters and offers which were originally wanted, and perhaps are still wanted, but not necessarily right now. Hotmail estimates that these emails represent 50% of all inbox traffic, and are the source of 75% of all spam complaints. The approach to combating Graymail represents a combination of techniques, and includes:

- A special category for the automatic placement of "newsletters"
- One-click unsubscribe facility
- Scheduled cleanups
- Flagging system for important emails
- User-created custom categories.

Whatever the approach, the core requirement is to maximise engagement with one's customers. However, engagement in itself is not the holy grail in terms of improved placement where smart inboxes are being operated. There are also some important caveats for email marketers to consider:

- The use of engagement data to determine inbox placement is becoming increasingly widespread, with these approaches now being made available at both individual mailbox level, as well as to achieve global prioritisation.
- Engagement data is being used both to influence inbox positioning (i.e. the question is one of "how high up the inbox") as well as inbox placement (ie "inbox vs bulk").
- Email marketers need to be careful that their definition of engaged may not necessarily be the same definition that the ISPs are using. Marketers will consider the data at their disposal, such as opens, clicks, conversions, or website activity. ISPs will be looking at metrics such as last log-in date, time spent in the email client, and whether behaviour resembles that of a real person, such as reading, deleting and even marking email as spam or not spam.
- Programmes that have been certified (see point 2.10 of the next section) will receive some protection against the mechanics that are used to operate smart inboxes. Certification reduces the filtering risk, and delivery rates will uplift as a result. That said, certification will not override any individual level filtering decisions.

Ultimately, email marketers who follow best practice, and who have the best sender reputation metrics will achieve Priority Status if their recipients interact and engage with their email programmes to a high level. The advantages to any organisation successfully reaching the Priority Inbox are clear as their emails would undoubtedly gain far more clicks and opens than emails listed without priority status.

[4] See http://en.wikipedia.org/wiki/Spamtrap

2. Ten steps to improved deliverability

2.1 Improve Data Collection

With the rapid rise in the importance of sender reputation, the quality of the email address data that is being used is absolutely vital. For this reason, there are several actions that an email marketer should take at the point of data collection that will improve deliverability on an ongoing basis:

- Strengthen the permissioning mechanism: There is a proven relationship between the permissioning mechanism that is used to sign up the new member, and their responsiveness. Positive opt-in (where the box is unchecked) is preferable to passive opt-in (where the box is pre-checked). Remember that a pre-checked opt-in box on its own cannot amount to consent to receive unsolicited commercial email under European legislation. While single opt-in (no confirmation email) remains the most commonly used permissioning mechanism, double opt-in (where a confirmation email is sent to the new subscriber with a link to activate the registration) provides 100% assurance in terms of the validity of the email address. Also, if your programme operates in certain EU territories (Germany, for example) double opt-in is in fact a mandatory requirement. From a best practice perspective, go for the strongest mechanism that your programme will support.
- Double entry of the email address: Many incorrect email addresses are simply the result of a "finger fumble" as the email is being typed in. This can be overcome by requesting the double entry of the address, with the two fields being cross-referenced against each other – it is highly unlikely that the same mistake will be made twice. This also eliminates a potential source of spam traps, as some ISPs track common mis-spellings ("hotmial" instead of "hotmail", for example) as a means of tracking whether appropriate list hygiene is being maintained.

  However, this approach does incur an additional overhead on the part of the subscriber, and may increase the risk that he/she might drop out of the registration process. Alternative approaches that can be used include:

  - Have the user confirm that the email address is correct at point of submission, or on the landing page that is produced after submission.
  - Make use of a welcome/validation email which will generate a non-delivery receipt (NDR) if the email address that has been supplied is incorrect.
- Send a validation email: Even if double opt-in is not being used as the permissioning mechanism, it is good practice to generate a confirmation/welcome email. This has some useful side-benefits:
  - Immediate validation of the new email address
  - Opportunity to positively reinforce the initial brand experience
  - Request to be added to the trusted senders list
  - Apply progressive registration approach to learn more about the new member.

In addition to the above techniques, there are also several third-party Application Programming Interface (APIs) that can be integrated into the data submission process to provide real-time email validation at point of entry. Two of these are referenced in the "Further Reading & Useful Links" section.

The subject of data collection is dealt with in greater detail in the Email Marketing Council's "Email Marketing Best Practice Guidelines" document. See "Further reading & useful links" for additional information.

2.2 Implement Authentication

With the explosion of "phishing" and "spoofing" emails (where a spammer adopts the identity of a legitimate domain owner), it is essential for the various parties who process emails to have a mechanism that proves that the email really has been sent by the party that it is claiming to originate from.

Responsibility for authentication will depend on whether the sender is using an Email Service Provider (ESP), or relying on its own email broadcasting infrastructure.

There are several approaches that an e-marketer needs to be taking to satisfy this requirement:

- Register a sub-domain or a custom domain specifically for the email activity. There are several benefits to be obtained from doing this:
    - The sub-domain can be linked to the broadcast server for SPF/Sender-ID needs
    - Generates increased recognition as users become familiar with the sub-domain
    - Can be added to the recipient's trusted senders list
    - Increased importance of domain-specific sender reputation monitoring
    - Domain-based certification solutions are being developed.
- Make sure that a Sender-ID/Sender Policy Framework (SPF) record is in place. This basically enables the receiving email server to carry out a lookup that validates whether the domain name that the email claims to represent is associated with the IP address that the email has been broadcast from. If this test fails, the email may be rejected. There are several good links that can be used to assist this process, which can be found in the further reading and useful links.
- Make sure that Domain Keys Identified Mail (DKIM) and Domain Keys are being utilised. This approach builds on Sender-ID/SPF (which validates the email's delivery path) by going one step further and authenticating each email message. This is done by including a signature key which is generated by the sender and included within the email header. The receiving email server will accept the email if it can successfully decode the key. This approach is popular with major ISPs such as Yahoo!, and also forms part of the checklist for Return Path certification (see point 2.10).

2.3 Monitor Your Sender Reputation

Sender Reputation is the single most important factor used to determine email acceptance by ISPs. A sender's reputation is monitored by a variety of factors and is linked either to the domain or the IP address from which the emails are sent or a combination of both.

ISPs often use external companies to provide sender reputation data so that they can screen emails against it. Many of these suppliers of sender reputation offer lookup facilities where users can enter an IP address and get a free report of their current sender reputation status. Some of the most well-known facilities include:

Vendor	Website Address
Sender Score (operated by Return Path)	www.senderscore.org
Senderbase (operated by Cisco Systems)	www.senderbase.org
AOL Postmaster	http://postmaster.aol.com/Reputation.php
McAfee TrustedSource	www.trustedsource.org

Typically, these sites will provide a high level classification of how the email traffic originating from that IP address is currently ranked. In the case of Sender Score, this is on a scale of 0 -100 (with 100 being a best case scenario), while in the case of Senderbase, AOL, and McAfee it's a traffic light-style system – "good, neutral, poor" or "green, yellow, red".

Users will also receive additional information on some of the key metrics that are being used to calculate the overall reputation score. These can include:

- Broadcast volumes: ISPs typically like to see "smoothed" broadcast activity rather than "spikes". If possible, spread activity over a wider broadcast window to achieve this
- Spam complaint notifications. Most ISPs operate spam complaint thresholds (typically between 2 to 3 complaints per thousand emails processed) with blocking becoming effective if these thresholds are exceeded. See point 2.6 (Feedback Loops) and Point 2.8 (Spam Complaints) for additional information
- Bounce back activity generated. Similarly, high levels of email delivery failure will also contribute to a poor reputation score. See point 2.5 (List Hygiene)

- Spam trap activity. These take two forms. Spam traps are email addresses that have been deliberately made available so that ISPs can track broadcasters who are using lists that have not been correctly permissioned. They can also be used to track recency – if an email address has been dormant for a long time, it may be co-opted and monitored on the premise that it should be de-selected if it is no longer active. See point 2.5 (List Hygiene)
- Blacklisting. This is a two-edged sword. Poor performance in the context of one or more of the metrics outlined above will be likely to result in one or more blacklisting. And once listed, there will obviously be negative implications for email deliverability. Point 2.7 (Blacklists) covers this subject in more detail.

2.4 Manage Your IP Addresses Carefully

As has already been explained in this document, sender reputation is an important concept for large volume email broadcasters (more than 100K emails per month). IP addresses used to send emails play an important role in determining a sender's reputation and therefore should be carefully managed.

Marketers who are broadcasting their emails through ESPs should be careful to understand what practices are being used to broadcast their emails. In some cases, senders will find that they are sharing IP addresses with other senders, in other cases they might be offered their own IP addresses. There is no right or wrong solution as different senders might benefit from different set-ups. When an ESP is using IP addresses shared across multiple clients, it's worth checking how carefully the IP addresses are monitored; if there are any acceptance levels in place to ensure only good senders are using those IP addresses, and who is responsible for monitoring those IP addresses. Equally senders, who prefer not to share IP addresses (and therefore reputation) with other senders, should take care to ensure that their own reputation is sufficient to ensure good delivery.

Particular care should be taken if a sender deploys a new IP address as (initially at least) it does not have a reputation score associated with it. The score builds as activity is tracked and metrics constructed. It is commonly held that the only thing worse than a poor reputation score is to have no reputation score at all. ISPs don't like surprises, and to be hit with a large tranche of email volume from a previously unknown IP address is almost certainly going to result in the broadcast getting blocked by one or more of the major ISPs. Senders who will only ever broadcast small volumes would generally be better served by a shared IP range where the volume is sufficient to gain a sending reputation.

For this reason, it is therefore important to "warm up" a new IP address. Some of the activities that can be used as part of this process include:

- Authentication. Make sure that all of the steps outlined in point 2.2 (Authentication) have been implemented.
- Throttling. Most email broadcast software now has the ability to "throttle" broadcasts, i.e. to restrict the number of emails sent to X thousand per hour. Initially, traffic being sent from a new IP address should be restricted to no more than a few thousand per hour – this figure can then be increased as the reputation score builds.

  Throttling can also be applied for individual ISPs. Several have a stated policy whereby the volume of email that they will process per hour is a direct function of the reputation score that is associated with the originating IP address.
- Clean addresses. If email addresses have been obtained from one or more data sources, or if it is possible to sort the addresses as a function of recency, then it makes a lot of sense to prioritise the broadcasting of the addresses that are least likely to complain/bounce back/contain spam traps/etc.

So – if one data source uses passive single opt-in while another data source uses double opt-in to collect its addresses, broadcast the double opt-in ones first. Similarly, addresses that have shown signs of life within the past 90 days are going to be more responsive than those that have been dormant for a year or more.

2.5 Practise Good List Hygiene

Good list hygiene is vital to the successful deliverability of an email campaign. To optimise list hygiene, a sender should consider the following points:

- Data Audit. Before the list is sent for the first time it should be screened to eliminate poor addresses. These could include:

    - Duplicate addresses
    - Known previous bounce back records
    - Invalid structure (no "@" sign etc.)
    - Junk entries (dfgdfgdfg@dfg.hj)
    - Common mis-spellings ("hotmial" instead of "hotmail")
    - Profanities
    - Potential harvested addresses ("sales@", "info@", etc.)
    - Foreign addresses (not incorrect, but potentially no relevance to local campaign).

- Bounce back management programme. A rigorous programme to remove emails that generate bounce back notifications should be implemented. Hard bounces (ie indicating permanent conditions) should ideally be removed with immediate effect. However, because some hard bounce notifications are in fact false positives, DMA best practice guidelines recommend using 2-3 hard bounce notifications as the recommended number before any action is taken.
- Soft bounces usually indicate temporary conditions, but should be removed if they continually fail to achieve successful delivery. For example, an address will be removed from selection if it generates 5 or more soft bounce notifications over a 28-day period. This may change depending on circumstances – for an academic institution; there could be a 60-day period to account for the summer holidays!
- Spam traps. These have been highlighted in point 2.3 (Sender Reputation), and can take the form of either "Honeypot" or "Retired/Recycled" addresses. They are not easy to identify as ISPs will never identify the actual spam trap address – that would be like gold dust for the spamming community.

  Instead, broadcasters and their clients should be adopting best practice standards in terms of how their data is being sourced, and using recency as a selection criterion. A good rule to observe is that spam traps never respond – they will not generate an open or a click-through response.

  Broadcasters should also sign up with programmes such as Microsoft's Junk Mail Reporting programmes, which will provide reporting on a 12 hourly basis of email activity containing spam traps. While it is not possible to identify the actual address, segmentations can then be introduced to quarantine the address.

  For further information on List Hygiene, please see Section 2.2 Data Hygiene of the DMA Email Marketing Council's Best Practice Guidelines.

2.6 Use Complaint Feedback Loops

Complaint Feedback Loops (FBLs) have been in existence for a number of years. They enable email senders to retrieve details of recipients who have complained (complainers) with their ISP/webmail provider when receiving the sender's email. Currently amongst others AOL, Yahoo!, Hotmail, and Comcast all operate a complaint feedback loop program, and in most cases these are mandatory requirements for programme certification (see point 2.10)[5].

Microsoft also offers its Smart Network Data Services (SNDS) tool which provides inbox data and notification of spam trap hits for Hotmail addresses, which is vital information for most B2C mailers. SNDS also flags up problem issues with Brightmail, a filter that is used around the world. See https://postmaster.live.com/snds for additional details.

Typically, complainers are identified through the webmail programs of the ISPs as those recipients who click the 'This is spam' button (or similar). The FBL provides the sender with the email addresses of the complainers so that they can exclude (unsubscribe) them from further mailings. They provide a key advantage to email marketers who wish to keep their list clean and avoid continuing to send to people who don't wish to receive their email programmes, yet don't take the time to unsubscribe.

FBLs are normally free to sign up for. The sender has to contact each of the ISPs, provide technical details about their sending systems. Once active, a daily feed of complaining emails will be sent back and can be excluded. If you are sending your marketing emails through an ESP, then they would normally need to set these up for you. In many cases, they would automatically do this for you, but it is something that you should check with them.

[5] See *"Further Reading & Useful Links"* for an extended list of vendors who offer FBLs

Although marketers may only think that they should sign up to the major FBLs, working on a premise of either: i) they don't have many subscribers at that domain and/or ii) it is not worth the effort, there is a case to be made against both the arguments. Effectively, the hosting companies are offering free data about the sources of spam complaints, and email programmes should take advantage of these opportunities.

Recent developments have also seen the addition of 'List Unsubscribe' and X-abuse Headers, which both enable recipients of emails to unsubscribe from those emails by contacting the company through which they receive their email. It follows a similar approach to a feedback loop, but rather than actually lodging a 'Complaint', the recipient can simply indicate their preference to be 'Unsubscribed' without the need to follow the sender's unsubscribe process (which may involve more steps). This is a great way to not only ensure those customers are removed from your list, but also to avoid them actually complaining and negatively impacting on your Sender Reputation.

2.7 Monitor Blacklists

Blacklists, sometimes known as Domain Name Server-based Black Lists (DNSBL), or Real-time Black Lists (RBL), are lists of IP addresses and/or domain information of senders who appear to be sending spam or unwanted email. They are compiled by a variety of organisations ranging from charitable organisations that campaign against spam, to commercial ISPs who keep their own lists to block unwanted mail. Many of these blacklists are made public and can be referenced by any organisation wishing to filter spam from their email traffic.

In simple terms, once a sender's information is listed on a blacklist, email will not be delivered if a receiver is referring to that blacklist when filtering inbound emails. There are several hundred blacklists in existence, although some are more influential than others and the impact of being listed is very much determined by the list upon which the sender finds himself. There are between 5 and 10 very important blacklists which are referenced around the world by many different organisations and spam filters. Links to these companies can be found in the "Further Reading & Useful Links" section.

Senders who find themselves listed on these critical blacklists will have severe delivery issues in many places. Any sender experiencing delivery problems would be well advised to check in the first instance to identify if they're being listed on any of the major blacklists. There are a number of websites (see list of Blacklist Operators in the Further Reading and Useful Links section at the end of the document) which provide a fast way to check if a listing appears.

Once a sender has determined that a listing has occurred then it will be necessary to contact the blacklist owner and try to get the listing removed. Each of the blacklist owners will typically provide information on their site to describe the 'de-listing process'. Senders using an ESP to manage their email broadcasting would require the ESP to handle this process. The blacklist owners often will seek reassurance that the infringement (cited as the reason for creating the listing) doesn't happen again. That might require the sender to provide evidence of good practice or simply be based on the acceptance of trust and assurance that no further infringements happen. Repeat offenders will find the blacklist owners very reluctant to remove the listing, and rightly so.

2.8 Reduce Spam Complaints

There is a direct correlation between spam complaints and subscriber engagement levels. Because of the algorithms that are now being used by inbox providers to determine placement and positioning, it is vital that the marketing mantra of "right message, right target, right channel, right time" is observed.

Disengaged subscribers will complain and, as described in section 6 above, spam complaints can have a very big impact on the delivery rates a sender achieves. Most ISPs and webmail providers base their spam filtering decisions to some extent upon the number of spam complaints seen from that sender. If a list owner or sender has an unusually high complaint rate (percentage of emails received by the ISP that are clicked as 'this is spam') they will start to consider emails from that sender as high risk, which in turn may lead to blockages.

There are many reasons why recipients would decide to mark your email as spam (complain):

- They didn't subscribe (i.e. you made a mistake in who you sent the message to)
- They didn't recognise you as the sender
- They forgot that they signed up

- You simply send too many emails - they weren’t expecting your emails so frequently
- The information in your emails isn’t interesting or relevant to them
- The unsubscribe mechanism is not easy to use – it’s quicker to click ‘this is spam’ than unsubscribe

There are two ways in which senders can reduce spam complaints:

a. Reactive approach
If you have feedback loops in place, complainers will be removed from your list over time. This approach will only work for certain ISPs and will do nothing to help reduce complaints where no feedback loop is in place. It may also be too late to avoid blockages occurring if you rely on feedback loops to reduce your complaints and complainers.

b. Proactive approach
A far more effective way to reduce complaints is to proactively take steps to avoid the complaints in the first place. The following tactics can all help to ensure the complaints are kept to a minimum.

   - Clear and easy to understand opt-in mechanism using double-opt-in or confirmed-opt-in methods for collecting email addresses
   - Employ prominent branding in the “From Address”, the “Subject Line”, and the “Preview Pane”. The more prominent the sender’s brand is in these areas, the less chance there is that the subscriber won’t recognise who the sender is, and hit the spam key instead
   - Clear and simple method for opting out – easily visible unsubscribe link, no small print or confusing language
   - An active reply address that goes to a monitored inbox so people who reply asking to be removed can be heard
   - Manage expectations – Make clear to your recipients when registering what you plan to send to them, how often, etc
   - Reduce your send frequency – too many emails can cause people to become frustrated
   - Give people choice – offering recipients the chance to tell you their preferences can dramatically reduce complaints

2.9 Conduct Pre-Broadcast Testing

In all aspects of email marketing it is a good idea to test. This is also true when trying to avoid delivery issues. Testing before sending with major ISPs will help spot any content related issues before the broadcast. Other factors, not necessarily related to delivery, can also be checked at the same time. For example, different webmail programmes can display emails in different ways – testing these to ensure your message renders correctly is always a good idea.

Many delivery issues can occur after a message has been sent or part way through the broadcast. For this reason it’s is a good idea to monitor the percentage of messages which are being delivered into the inbox versus the junk folder with the major ISPs.

There are a number of tools available (both through ESPs and delivery specialists such as Return Path & Pivotal Veracity) which check this for you. They work by seeding campaigns with a large number of sample addresses for each ISP and then automatically login and check whether they were delivered or not.

Using these results, the tools can provide an estimation of the ‘Inbox placement rate’ or ‘ISP acceptance rate’ (not to be confused with delivered rate). By monitoring your inbox delivery rate you can quickly spot when blockages might have occurred.

Pre-broadcast testing touches many elements of email best practice. See the following DMA white papers for further insight on this topic:

- Email Creative
- Data Analysis & Segmentation
- Split Testing

2.10 Accreditation Schemes

Accreditation schemes establish a sender's credentials, and then confer a range of benefits such as reduced throttling restrictions, preferential treatment by spam filters, and auto-enablement of images. They typically operate through a process of the sender paying a fee, and then undergoing a verification process in order to prove that they are a good sender and follow best practice methods for sending bulk email communications. Once the accreditation has been achieved, senders then benefit from being able to bypass key spam filters, as well as having images readily available for users to see without the need for downloading.

The best known of these schemes is Return Path Certification (originally known as the IronPort Bonded Sender Program, and more recently as Sender Score Certified), which doesn't charge users a per email fee, but which does involve an annual subscription fee. The scheme works by a process of verification to ensure the sender's practices are of a high enough standard to be accredited as a good sender. Once accepted on to the scheme the sender is then white-listed with all of the participating ISPs and domains including Hotmail, Yahoo! and BT Internet.

Currently, certification operates on the basis of the IP addresses that the sending activity takes place from, necessitating that a unique IP address/es is dedicated only to the sending of the certified email traffic. However, it is predicted that this will change, and that domain certification – whereby the sender's domain rather than specific IP addresses is the entity that is certified – will become a reality in the near future. Some vendors (such as Cloudmark, for example) already calculate sender reputation as a function of domain rather than individual IP address, and it will be logical for certification solutions to be aligned with this approach.

Further reading & useful links

The following section provides a list of useful documentation and website links that readers can follow for further information on the points that have been dealt with above.

Resource	Link
Deliverability	
Return Path	http://www.returnpath.net/landing/globaldeliverability2h11/
Blacklist Operators	
Spamcop	www.spamcop.net
Spamhaus	www.spamhaus.org
MAPS	www.mail-abuse.com
SORBS	www.sorbs.net
Authentication	
Microsoft	www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/
Open SPF	www.openspf.net
DKIM	www.dkim.org
Domain Keys	http://help.yahoo.com/l/us/yahoo/mail/classic/context/context-07.html
Blacklist Monitor	
Debouncer	www.debouncer.com
Return Path	http://www.returnpath.net/commercialsender/monitoring/
Monitor Your Sender Reputation	
Sender Score (operated by Return Path)	www.senderscore.org
Senderbase (operated by Cisco Systems)	www.senderbase.org
AOL Postmaster	http://postmaster.aol.com/Reputation.php
McAfee TrustedSource	www.trustedsource.org
Complaint Feedback Loops	
AOL	http://postmaster.aol.com/Postmaster.FeedbackLoop.php
Yahoo!	http://feedbackloop.yahoo.net/
Hotmail	https://support.msn.com/eform.aspx?productKey=edfsjmrpp&page=support_home_options_form_byemail&ct=eformts&scrx=1&st=1&wfxredirect=1
Comcast	http://feedback.comcast.net/
Microsoft SNDS	https://postmaster.live.com/snds
Return Path Feedback Loop Setup Guide	http://www.returnpath.net/resources/archives/Return%20Path%20Feedback%20Loop%20Set%20Up%20Instructions.pdf

FBLs are also offered by vendors such as Rackspace and Tucows.

Improve Data Collection

DMA Email Marketing Council Best Practice Guidelines (June 2007)	http://www.dma.org.uk/toolkit/email-marketing-best-practice-guidelines
Real Time Email Address Validation	http://biz.freshaddress.com/RealTimeEmailAddressCorrection.aspx http://www.towerdata.com/services/web/email_validation.html

Conduct Pre-Broadcast Testing

Return Path	http://www.returnpath.net/commercialsender/monitoring/
Pivotal Veracity	http://www.alterian.com/pdf/Pivotal_Veracity_UK_061109.pdf
DMA Email Creative White Paper	http://www.dma.org.uk/toolkit/email-creative
DMA Data Analysis & Segmentation White Paper	http://www.dma.org.uk/toolkit/guide-data-analysis-and-segmentation-%E2%80%93-white-paper
DMA Split Testing White Paper	http://www.dma.org.uk/toolkit/guide-split-testing-%E2%80%93-white-paper

Get Certification

Return Path	http://www.returnpath.net
Return Path Certification	http://www.returnpath.net/commercialsender/certification

General Resources

Email Marketing Council blog	http://www.spamcop.net
Messaging Anti-Abuse Working Group	http://www.maawg.org

About the DMA

The Direct Marketing Association (DMA) is Europe's largest professional body representing the direct marketing industry. With a large in-house team of specialists offering everything from free legal advice and government lobbying on direct marketing issues to research papers and best practice, it is always at the forefront of developments in the industry.

The DMA protects the direct marketing industry and consumers. It promotes the highest standards through self-regulation and lobbies against over-regulation. The DM Code of Practice sits at the heart of everything we do – and all members are required to adhere to it. It sets out the industry's standards of ethical conduct and best practice.

Our 10 DMA Councils/Board Committees cover the whole marketing spectrum – from the digital world of social media and mobile marketing to the 'real' world channels of door drops and inserts. The Councils are made up of DMA members and regularly produce best practice and how to guides for our members.

We also have a packed calendar of conferences, workshops and discussions on the latest topics and best practice, and 80% of them are free for members and their staff.

As the industry moves on so do we, which is why we've recently launched a number of new services for our members – a VAT helpline, a Social Media Helpdesk and an IP Protection Service.

Visit www.dma.org.uk regularly to keep up to date with all our services.

we are the dma

About Return Path

Return Path is the global leader in email deliverability solutions, helping over 3,000 of the world's best-known brands to get their legitimate email delivered and keep fraudulent email out. We work in conjunction with Email Services Providers (ESPs) to: monitor your deliverability, get into the inbox at hundreds of ISPs, increase email response rates, manage email sender reputation and protect your brand against spoofing, phishing and other abuse.

Return Path's powerful email monitoring and protection tools quickly identify problems interfering with email campaign success, so you can implement the right solutions to bring tangible improvements.

We help marketers get through to target audiences. Our customers include leading global brands who have seen real improvement in their email ROI through our solutions including Twitter, Groupon, Citrix Online and Renault.