



Interactive Advertising Bureau Marketer & Agency Guide to Email Deliverability

Table of Contents

Executive Summary	3
Why should I care about deliverability?.....	3
Deliverability Defined.....	3
Main causes of Deliverability issues	4
FILTERS - How Receivers Filter.....	4
How do I know if I have deliverability problems?	6
Measurement	7
Improving Deliverability.....	8
FILTERS - How You Control Filtering.....	8
About IAB.....	13
About IAB Email Committee	17
Footnotes.....	13

Executive Summary

This document reviews the definition of deliverability, its history, and the impact on marketers. The current causes of how to measure and monitor and how to resolve deliverability issues are also addressed. It is important to recognize that the deliverability landscape changes multiple times per year and the best practices for monitoring and resolution change with it.

Why should I care about deliverability?

Deliverability challenges can cause your email messages to have images and links disabled, to be placed in a Junk Mail folder, or to be discarded before the recipient ever sees them. This means lower open rates, lower clickthrough rates, lower conversions, and lower revenue.

More than 20% of legitimate marketing messages are incorrectly identified as spam by server and client level spam filtering, so chances are that if you aren't watching it closely then you have deliverability problems.

Unfortunately, few marketers today can expect to achieve perfect deliverability. For many, deliverability can be a confusing and painful issue. But by configuring things correctly from the start, adhering to best practices, and monitoring industry trends you can feel confident that you are achieving the highest relative deliverability for your industry, brand, and type of messaging.

Deliverability Defined

Deliverability is a household term for email marketers today. But this has not always been the case. Before diving into the definition, it is important to look at the chain of events that brought us to today.

As popularity of email as a method of communication grew over the past 10 years, the volume of email being sent increased exponentially. Today over 60 billion emails are sent every day. This increase was accompanied with an increase in SPAM attacks. Between March 2001 and August 2003 alone, unique SPAM attacks increased over 700%. Today, approximately 80% of total email traffic today is SPAM. SPAM at these volumes created inboxes flooded with unwanted messages and subsequently lowered consumer confidence in email. Challenged to keep customers happy, ISP's implemented more strict and complex filtering logic on inbound message to block spam. Along with filters, new white listing practices, and new junk/bulk folders were created. Initially, ISP filtering logic and practices were not publicly available and did not come without impact on email. Early ISP filtering practices created a false positives challenge in which legitimate email was often marked as SPAM and subsequently not delivered at all. With little visibility of the exact details behind ISP filtering,

Marketer & Agency Guide to Email Deliverability

marketers started seeing negative trends in the performance of their email campaigns due to the change in ISP behavior. The impact observed included but is not limited to:

- missing messages,
- lower open rates,
- lower response rates, and
- lower conversion rates.

As part of an effort to better understand the root of these delivery and performance changes, email marketers, ISP's, and vendors started working together to better understand SPAM volumes, ISP filtering, and their impact on email. In 2003, "Deliverability" was born.

Although the email deliverability landscape has started to stabilize, it is a constantly changing battleground that continued to change past 2003 and continues to change today. In 2004, CAN SPAM federal legislation was launched, and blueprints to solve SPAM issues were developed. 2005 represented a significant shift towards creating an environment that requires marketers to have more control over their deliverability. Specific movements such as adoption of authentication technologies, and reputation services have been the leading drivers.

Defined, deliverability represents the ability of an email marketer to consistently deliver email to recipient's inbox with full HTML of Text functionality as indicated by the recipient in his/her preferences. It is important to note that deliverability is not a metric, there are metrics that help you track your deliverability and delivery success that are covered later in this document. It is also important to note that Deliverability is relative. Marketers should focus on how are other people like "me" are performing.

Deliverability has grown into its own market within the email industry. A market that has its own experts, consultants, technology providers and following.

Main causes of Deliverability issues

It is important, though, to first understand what will get you filtered, and how you control those factors.

FILTERS - How Receivers Filter

Before you can fix problems, you need to know what causes them, and what those who control delivery are looking for from you.

There are **seven primary filtering methods** used by ISPs and corporate system administrators as they deal with the deluge of spam hitting their servers every minute. Those are:

Marketer & Agency Guide to Email Deliverability

Public Blacklists:

Several organizations like Spamhaus and Spam Cop keep lists of IP addresses linked to suspected or known spammers, and make them public for ISPs and others to use in screening out spam.

Private Blacklists:

ISPs and some corporate system administrators also keep their own domain specific list of IP addresses for suspected spammers. These are typically based on complaints received from subscribers, but they can also be based on other criteria like unknown user rates and server configuration issues.

Fingerprinting

The most commonly known fingerprinting system is Brightmail. These systems work by filtering known spam messages after matching them against creative or chunks of text that has either generated previous complaints, or was delivered to spam trap addresses. It is becoming more and more common for URLs to be the text that gets fingerprinted – both AOL and IronPort utilize this practice extensively.

Spam Traps:

SpamCop, Brightmail, Lashback and Hotmail all monitor spam traps. Spam Traps are special addresses created to attract spam – they don't go to a person – instead they are logged and monitored. Some spam traps are old defunct user accounts that have not been used in many years while others are special addresses created just to be spam traps. Lashback uses seeding extensively to monitor CAN-SPAM compliance with suppression lists.

Machine Learning-based Content Filters:

These filters are the one everyone thinks of when blocking is based on words and phrases. Machine learning (Bayesian) filters can be based on the content in the email body or header. Body details such as HTML coding, design, links syntax, and content can all be used within Machine learning filters. This is a primary technique of Spam Assassin and is also widely used by client-side spam filters (Outlook, Apple Mail, AOL) that learn from users clicking “this is spam”. Corporate Filters, and consumer based ISPs have different approaches, scoring formulas.

Server Configuration:

Certain server configurations open you up to instant blocking. These include not having a reverse DNS, misconfigured SenderID or Domain Keys, or having open relays or open proxies.

Volume Cap:

Some ISPs, like Yahoo! or Earthlink, may shut down sending connections when resource demand gets too high. Be mindful of your number of connections or messages per connection so they don't exceed their thresholds. Volume caps in most cases aren't just volumetric, they are a combination of the newness of your IP address, your reputation, number of complaints exceed a threshold as well.

Challenge Response:

Some systems require a reply to a challenge message, which basically proves you are a real person and prevents automated messages. After confirming that you are a real person, your email address is added to the recipient's address book so that you can bypass future challenges.

How do I know if I have deliverability problems?

Before focusing on how to improve deliverability it is important to be able to identify if you are having problems first. To identify if you are having deliverability problems:

Establish Benchmarks

Find out what the expected rates are for your industry, the strength of your brand, and the type of messages that you are sending so that you know how you compare.

Monitor your Program Performance

Watch your bounce rates, open rates, click-through rates, unsubscribe rates, and complaint rates on a per mailing basis. When you see something strange, break it down by domain and see if it's a problem with one domain in particular or spread across all domains evenly. Make sure you actually look at the raw bounce codes – some are hard to read but many are very helpful. Watch your rates as they change over time so that you can detect relative ups and downs.

You will also want to monitor actual inbox delivery rates, which is most assuredly not the number of messages sent minus the number that bounce back. The easiest way to do this is through a deliverability monitoring company which will seed your list with addresses across the various receivers and give you a report by campaign of the percentage of messages that arrive in the inbox, get diverted to the junk folder or fail to appear at all. You can also do this manually by signing up for accounts across ISPs and monitoring those accounts. The manual approach is generally not nearly as accurate as an automated system, but may be a good starting point for some mailers. Some email service providers offer automated deliverability monitoring as part of their package. But buyer beware - due diligence to be sure this is a true deliverability solution (and not a report on bounces) is important.

Marketer & Agency Guide to Email Deliverability

Register for feedback

Make sure you're monitoring as much information as you can gather. Promptly remove users who unsubscribe or complain.

Places to get feedback include:

- Abuse.net - <http://www.abuse.net/addnew.html>
- AOL - <http://postmaster.info.aol.com/fbl/index.html>
- Lashback – <http://www.lashback.com/>
- Microsoft SNDS – <http://postmaster.msn.com/snds/>
- SenderBase – <http://www.senderbase.org/>
- SenderScore - <http://www.senderscore.com/manageYour.php>
- SpamCop - <http://www.spamcop.net/fom-serve/cache/94.html>
- TrustedSource – <http://www.trustedsource.com/>
- United Online - <http://www.unitedonline.net/postmaster/whitelisted.html>

Measurement

Deliverability itself is not a metric, nor is it something that can be tracked through a single metric. A series of metrics are used to measure deliverability. Metrics include everything from bounce, delivery, and inbox figures to various open, click, and conversion rates.

Companies using email to drive response must look at a full-picture view of their program if they want to improve their current performance rates. Traditionally bounce rate was the key delivery metric, but instead of relying solely on bounce responses, you should track your delivery by monitoring the additional delivery metrics provided as well as standard click, open, and conversion performance at the program and domain level.

To further complicate things, there is no industry standardization on the exact metrics to use or the formulas and methodologies used to track deliverability. In today's market it is difficult to differentiate between one source of "delivery" rates against another. It is not uncommon to see email service providers touting rates as high as 98 and 99% delivery rates. Although most providers provide transparency into the methodology used to calculate their rates, the lack of consistency creates challenges. Improving marketer's abilities to understand, track, monitor, and improve deliverability, standardization within the industry is needed. It is also helpful to note that the industry is beginning to refer to "Confirmed Opt-in" as a "Closed-loop Confirmation Process".

Be sure to clearly understand the formulas used by your email technology when reviewing program success. Also, be sure to read the foot notes of the industry email trend reports.

Improving Deliverability

Every company sending large volumes of commercial or transactional email struggles with a hidden issue: email deliverability. Aware of it or not, nearly 20 percent of email gets blocked or filtered by ISPs and corporate system administrators. Whether email is sent in-house or through an ESP, non-delivery erodes response rates and program effectiveness.

To determine how email deliverability affects your email program, there are several things you need to do:

- Understand the factors that contribute to blocking & filtering.
- Monitor your program delivery to learn the extent of problems.
- Uncover the root causes of your specific issues.
- Ensure your technical infrastructure meets required standards.
- Build relationships with ISPs to help resolve delivery issues.

FILTERS - How You Control Filtering

There is a tendency to point the finger to everyone other than in the mirror when looking at blocking issues. The truth is, though, that you control nearly every facet of blocking and filtering that happens after you hit the “send” button on your campaigns. There are five areas within your control that contribute to filtering:

- Complaints
- Content
- Unknown Users
- Server Configuration
- Spam Traps

Complaints:

The number of people who complain to ISPs and spam watch groups about your email can be detrimental to your email program. The first line of defense is to make your email program so relevant that it is at the opposite end of the spam spectrum.

According to a 2004 DoubleClick study, 72% of people think that hitting the “this is spam” button in their email client is the best way to unsubscribe from a list. This means that every time your customers decide they don’t want your email, you are susceptible to complaints at the ISP level – and the ISPs make this easy with very prominent “report spam” buttons.

You can minimize complaints by following specific best practices. Follow this checklist to make sure your complaints are kept to a minimum. Then, make sure you keep track of your complaints and correct issues causing them.

Marketer & Agency Guide to Email Deliverability

Some resources available to help you keep track of complaints to ISPs are:

- AOL Feedback Loop
<http://postmaster.info.aol.com/fbl/index.html>
- United Online Feedback Loop
<http://www.unitedonline.net/postmaster/whitelisted.html>
- SpamCop
<http://www.spamcop.net/fom-serve/cache/94.html>
- Abuse.net
<http://www.abuse.net/addnew.html>
- Lashback
<http://www.lashback.com>

Checklist: How to Reduce Complaints

Even messages sent with the highest permission levels and best practices will often generate some spam complaints. Based on your industry and the type of spam complaint (SpamCop, AOL, SNDS, etc.) you should set an acceptable complaint rate and monitor it closely. If you start to generate too many complaints, there are a number of steps you can take to improve the user experience and reduce the likelihood that recipients will click “this is spam”.

Manage your registration process so that you can meet future expectations.

- Give subscribers a positive choice.
- Give them a good idea of what they will receive.
- Make choices granular.
- Use the most conservative permission standard you can.
- Send a welcome message.
- Give instructions on how to add your email to the address book.
- Use the highest permission standard you can support.

You can make a business case for verified (“double”) opt-in; Confirmed opt-in at minimum.

- Fewer unsubscribes.
- Fewer complaints (more delivery).
- But: Smaller list.

Marketer & Agency Guide to Email Deliverability

Always respect unsubscribe requests.

- Make it easy to unsubscribe.
- Make sure your unsubscribe works.
- Process unsubscribe requests before sending subsequent mail.

Ensure your content/program relevancy is on target – it impacts behavior.

- Appropriate mail frequency.
- Stay consistent.
- Use customization and personalization.
- Target messaging.

Conduct complaint analysis- where are they coming from?

- New subscribers? Points to relevancy issue.
- Particular data source? Kill or re-permission bad data.
- Non-responders? Stop mailing!
- Creative? Re-think creative and copy.
- Frequency? Lessen or increase frequency as needed.

Content:

Make sure your content is free of spam filter triggers before you send a campaign. Test creative before sending campaigns to make sure it does not fail the most-used filtering applications. You can't assume that avoiding words like "free" will ensure your delivery. Sometimes the most innocuous words – and uncommon ones – can trip up your best efforts. The only way to ensure that your content doesn't trigger a block is to test it in a "spam lab," available through deliverability service providers.

Unknown Users:

ISPs block domains in part based on the number of "unknown user" errors generated when sending mass emails. Keeping your email list clean and current will help lower the percentage of bad addresses on your list resulting in "unknown user" codes at ISPs. Some things you should do:

Use a bounce algorithm that will remove "all addresses experiencing permanent failure" addresses from your file promptly, ending both "inline" and "message" bounces.

Marketer & Agency Guide to Email Deliverability

- Process your file through a consumer-reported Email Change of Address service.
- Run your file through a list hygiene service.
- Require double entry of addresses for accuracy.
- Check addresses for RFC compliance & ISP standards.
- Send a welcome message and pull bounces off immediately.

Server Configuration:

Technical triggers, such as having no reverse DNS record, are easy to miss but will lead to blocking by ISPs instantly. Make sure your email operations team knows all the ins and outs to setting up your email server, including the new rules around authentication.

Spam Traps:

If your list has spam trap addresses on it, you're doomed. Data partners impact this, as do your own bounce algorithms and list hygiene practices.

Vet data partners carefully, as data collected from third parties puts you at most risk for bad addresses being added to your file.

- Send a welcome message to all new subscribers; Remove bounces or complainers immediately.
- Use some sort of 'Bot' submission "trip wire" to make sure that no one maliciously adds bad data to your file.
- Regularly cull out old, non-responsive addresses from your list. The definition of old will vary by business, but as a starting point, consider cleaning out any address that has not opened or clicked in the past 90 days.

All of these things are symptoms of your program practices and are things you can improve upon to ensure inbox reach.

Email Authentication:

Authentication solutions are technology protocols that establish the true identities of senders and allow for the development of a sender's email reputation.

Two main approaches to determining authenticity of email exist today: IP based solutions and Crypto-based solutions. Sender ID, a combination of Microsoft's Caller ID and Sender Policy Framework (SPF), is the leading IP based authentication solution. With Sender ID, authentication is achieved by verifying that the server sending email for a particular domain is authorized to do so.

- Domain Keys Identified Mail (DKIM), a combination of Yahoo!'s Domain Keys and Cisco's Identified Internet Mail (IIM) is the leading crypto-based solution. With DKIM, authentication is achieved through the use of digital signatures.

Marketer & Agency Guide to Email Deliverability

Email marketers should support SPF, and SenderID within all messages. If supported by their MTA's marketers should also support DomainKeys or DKIM.

More information on Authentication solutions can be found at:
http://www.iab.net/standards/Auth_Rep_Accred_Guide_Final_Rev1.pdf

- Microsoft Sender ID – http://www.emailauthentication.org/docs/SIDF_Overview_Brochure_v3.1.pdf
- Sender Policy Framework – <http://spf.pobox.com/>
- Yahoo! Domain Keys - <http://antispam.yahoo.com/domainkeys>
- Cisco Identified Internet Mail – <http://www.identifiedmail.com/>
- <http://www.deliverability.com>
- <http://www.emailauthentication.org/resources/>
- <http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx>
- <http://www.deliverability.com>

Accreditation Services

Accreditation services are 3rd-party programs that certify sender policies and practices and contribute to a sender's email reputation.

More information on available accreditation services can be found in "A Marketers' Guide to Accreditation, Reputation, and Authentication Resources", published by the IAB & ESPC.

http://www.iab.net/standards/Auth_Rep_Accred_Guide_Final_Rev1.pdf

Reputation Services

Reputation services monitor and gather all available data intelligence on senders and aggregate a global reputation score

More information on available reputation services can be found in "A Marketers' Guide to Accreditation, Reputation, and Authentication Resources", published by the IAB: ESPC.

http://www.iab.net/standards/Auth_Rep_Accred_Guide_Final_Rev1.pdf

Deliverability Monitoring Technology & Services

Deliverability monitoring technology and services can help identify, track, monitor, and improve deliverability. These services have grown to do more than merely check to see if it arrived or was filtered and are offered in a wide range of flavors. Solutions can be as small as a feature on hardware and as large as full service consulting agencies.

About IAB

Founded in 1996, the Interactive Advertising Bureau (IAB) represents over 250 leading interactive companies that are actively engaged in, and support the sale of interactive advertising. IAB members are responsible for selling over 86% of online advertising in the United States. On behalf of its members, the IAB evaluates and recommends standards and practices, fields interactive effectiveness research and educates the advertising industry regarding the use of interactive advertising. For more information, please visit www.iab.net.

About IAB Email Committee

The Email committee is a forum for direct marketing media professionals of IAB member companies whose objective is to support this medium as a valuable channel to advertisers and their agencies. The committee will work to address all performance marketing related issues and recommends solutions, standards and educational tools as needed. The committee will deliver these objectives through industry research, case studies and stakeholder education.

Email Committee Members

Alexa Wriggins, IDG	Kristen Terzo, GSI Commerce
Andrew Pancer, About, Inc.	Kristi Thomas, Verizon Superpages.com
Anita Absey, Return Path	Kristina Behr, MSN
Annette Barnes, Expedia	Mai Wah Cheung, Univision Online
Bennet Kelley, ValueClick, Inc.	Michael Hurt, MSN
Brad Bacon, Weather Channel	Michael Stuart, CondéNet
Brian Seskin, iVillage, Inc.	Michele Frost, Critical Mass
Cliff Bates, Walt Disney Internet Group	Missy Barnstein, Advertising.com
Craig Swerdloff, Return Path*	Ron Nielsen, Vendare Media
David Baker, Agency.com	Sarah Lumbard,
Eric Budin, Comcast	Washingtonpost.Newsweek Interactive
Erik Kokkonen, CNET Networks, Inc.	Sasha Koren, New York Times Digital
Erin Miranda, Weather Channel	Sean Quick, Mediaplex (ValueClick)
Interactive	Susannah Manheim, Q Interactive
Jeff Brough, TMP Directional Marketing	Sylvia Marino, Edmunds.com
Jeff Peterson, QuePasa.com	Talib Morgan, Actuan, LLC
Joshua Baer, Datran	Todd Taplin, Yahoo!, Inc.
Karen Nugent, Vendare Media	

Special thanks to Sean Quick, Anita Absey, Joshua Bear, David Baker along with Jim Campbell and the ESPC for their time, talents and contributions to the development this document.

* Committee Chair

Footnotes

- Return Path – Beyond Clicks, Opens & Bounces: Metrics that reveal the path to optimal email performance. White Paper
- Return Path – Deliverability 101 White paper
- Pivotal Veracity – “False Positives” Study
- Strong Mail – Authentication White paper
- NAI ESPC – Authentication / Reputation providers
- <http://www.emailauthentication.org/resources/>
- Jupiter Research
- Deliverability.com