The Ultimate Guide to Email Deliverability

Return Path
FROM VALIDITY

Table of Contents

Chapter 1
Email Deliverability Defined

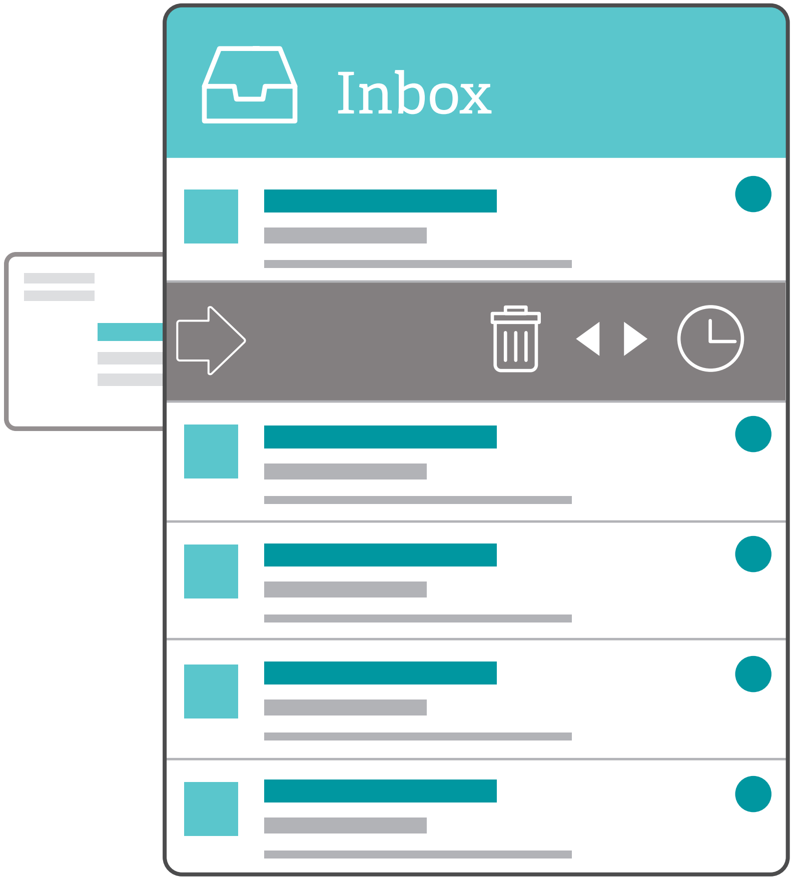
Deliverability is the brass ring that every marketer strives for, but it's surprisingly difficult to define. Try Googling the term and your results will leave you more confused than when you started.

Part of this disconnect is due to a single misleading metric: delivered rate. The name "delivered rate" implies that it measures your brand's deliverability—your ability to get into the inbox of your subscribers. But what it actually measures is the amount of sent email that received neither a hard nor soft bounce.

Many marketers mistakenly feel secure in their ability to reach subscribers when they have a high delivered rate. However, delivered email (i.e., email that didn't bounce) could land in the inbox, the spam folder, or get blocked.

You might be thinking. "What? My delivered emails are going into the spam folder? But I'm not a spammer!" You might be right, but the spam folder is not just for spammers. In order to protect users from spam and other malicious email, mailbox providers analyze various aspects of both the sender and the incoming message to determine what actually belongs in the inbox.

In the coming chapters, we'll dig into the various aspects of deliverability, how mailbox providers distinguish the good from the bad, and what every marketer can do to make sure their campaigns actually land in the inbox.



Chapter 2
The History of Spam

The definition of spam has been debated ever since the early days of email and the Arpanet back in the 1970s. The most commonly accepted definition of email spam is Unsolicited Bulk Email (UBE), or messages sent to a large number of recipients without permission.

Spam is in the eye of the beholder

Of course, this simple definition doesn't tell the whole story. Some argue that explicit permission isn't needed if a prior business relationship exists. And to confuse matters further, some consumers refer to all marketing email as spam—just as they label all bulk postal mail "junk mail."

This fuzzy definition of spam led to the development of the "This is Spam" button in AOL mail, which helped its spam filters determine what users thought was spam. Today, even the spam button doesn't clearly denote what is spam as many people also use it as a substitute for unsubscribing from unwanted email.

Clearly, spam is in the eye of the beholder. If a recipient believes that the email is unwanted and sent without permission, the email is considered spam. However, if we look at the intentions of the sender, the definition of spam becomes a little more clear. If someone hijacks a PC to send to millions and millions of email addresses that were bought, it's spam. If the intention is to send marketing emails to a customer, it's email marketing.

Where did spam originate?

Email was created in 1971 by Ray Tomlinson as an effort to reach colleagues who didn't answer their phone. It wasn't until years later that the first "spam" email was sent.

In 1978, Gary Thuerk sent a message to hundreds of people promoting a new computer model from the Digital Equipment Corporation through the Arpanet system. The reaction to the message was mixed. Some viewed the email as obtrusive, but some found the email relevant and didn't think it was a big deal. Thuerk stated he sold "$13 million or $14 million worth" of computers, making him both the "father of spam" and the "father of email marketing."

The term "spam" became widely used in the 1980s after a comedy sketch by Monty Python. In the sketch, the word "spam" was used repeatedly to describe the offerings on a restaurant menu which annoyed the patron who didn't like Spam. The term was adopted by early internet users and came to mean repeatedly posting the same message or trying to discourage legitimate communication. When internet use exploded in the 1990s, it opened the door for early spam pioneers to send their unsolicited email messages to an unsuspecting public.

While spam volumes have been decreasing since 2012, most email sent today is still spam. According to Return Path's *2014 Sender Score Benchmark Report*, spam comprises more than 70% of all email.

Chapter 3
How Spam Filters Work

There are countless articles on the web entitled, "How to Avoid Spam Filters." The problem with most of these articles and their advice is that they're based on the false premise that it's possible to avoid spam filters.

Spam filters are part of the process. If you send email, it will be filtered—either to the inbox, a categories tab, a spam folder, or it will be blocked completely. Filter technology plays a massive role in the success of your email campaigns. That's why, at Return Path, we encourage our clients to embrace spam filters, learn how they work, and understand how mailbox providers use them.

What is a filter?

Email filters organize email according to specified criteria. Originally, filters were designed primarily to identify spam and block it or place it in the spam folder. Today, some mailbox providers use email filters to categorize messages for inbox-organization purposes (e.g., social media and newsletters).

Why do mailbox providers filter email?

Mailbox providers have strong motivations to use spam filters, whether they build their own system, leverage third-party spam filter technology, or use a combination of home-grown and partner anti-spam solutions. Spam is annoying, no doubt, but it can also be dangerous. Malware and phishing are hugely profitable for scammers and can be costly for mailbox providers' customers, as well as the mailbox providers who face intense market competition. Practically speaking, spam filters drastically reduce the load on server resources, considering that 70% of all mail sent globally is spam.

As a message traverses from the sender to the subscriber's inbox, various types of filters can influence deliverability and inbox placement:

Gateway spam filters are physical servers that are installed at the border of a company's network, and serve as a mailbox provider's first line of defense in preventing spam. All mail attempting to come into the company must pass through this "gate" before it can enter the system. This spam filter learns what to deem as spam based on all the email coming into the company, which means it has less email data to learn from than a hosted spam filter. Examples of gateway spam filters include Cisco's IronPort and Barracuda.

Third party (or hosted) spam filters are companies that have developed a proprietary method of using content and reputation metrics to distinguish spam from legitimate mail. Third party spam filters can influence filtering decisions at the gateway or after a message is accepted through the gateway (i.e., spam or inbox placement). Since these spam filters have a large book of clients using their service, they have a broad scope of information to use in determining whether to deliver to the inbox, spam, quarantine folder, or block the message completely. Third party spam filters can include technology that is integrated by vendors directly into their own products. Examples of third party filters spam filters include Cloudmark and MessageLabs.

Desktop spam filters are a version of third party spam filters that live on the end user's computer. They are highly customizable by the individual, so they can be among the more difficult filters to pass through. An example of a desktop spam filter is Outlook, which uses Microsoft's anti-spam filter SmartScreen to help filter email. SmartScreen uses the feedback from Windows Live Hotmail users to help distinguish legitimate emails from spam.

The basics of filter technology

Spam filter technology may be placed on both inbound email (email entering the system) or outbound email (email leaving the system). Mailbox providers use both methods to help protect their customers. Senders may encounter both types of filters but are mostly concerned with inbound filters.

Both outbound and inbound filter methods use algorithms, heuristics, and the more advanced form of heuristics known as Bayesian as part of their filtering technology. Algorithms in this context are rules that tell a program what to do. Heuristics work by subjecting email messages to thousands of predefined rules (algorithms). Each rule assigns a numerical score to the probability of the message being spam.

An equation might look like this:

$Pr(S|W) = Pr(W|S) \cdot Pr(S)$

$Pr(W|S) \cdot Pr(S) + Pr(W|H) \cdot Pr(H)$

$Pr(S|W)$ is the probability that a message is spam, knowing that the word “Viagra” is in it.

$Pr(S)$ is the overall probability that any given message is spam.

$Pr(W|S)$ is the probability that the word “Viagra” appears in spam messages.

$Pr(H)$ is the overall probability that any given message is not spam (is “ham”)

$Pr(W|H)$ is the probability that the word “Viagra” appears in ham messages.

The main types of filtering analysis

Mailbox providers look at three main aspects of mail when making filtering decisions:

The source of the mail (details in Chapter 4)

The reputation of the sender (details in Chapter 5 and Chapter 6)

The content of the mail they send (details in Chapter 7)

Source:

Spammers often attempt to “game” reputation systems by using multiple (and constantly changing) IP addresses or domains. However, spam filters look at factors such as sender authentication, sending permanence, and the age of the IP addresses and domains in their filtering decisions.

To that end, email sent from new IP addresses and domains is treated with caution by mailbox providers. Senders that change IP addresses and domains infrequently and use authentication techniques can be seen as more trustworthy, which may lead to a stronger sending reputation.

Reputation:

The reputation of the sender is calculated using algorithms and heuristics, leveraging millions of data points and hundreds of parameters. A “reputation score” can range from 0 to 100 (Return Path’s Sender Score), from -10 to +10 (IronPort’s SenderBase), or apply categorical scoring like AOL’s: undisclosed, neutral, good, and bad. Based on the strength of the reputation score, mailbox providers will make filtering decisions about the email coming from a sender.

Reputation-based filters can automatically apply the mailbox providers’ mail flow policies based on the reputation score of the sender. As the filter receives inbound mail, a threat assessment of the sender is performed. Some of the parameters leveraged to generate a reputation score are:

Complaints

Spam traps

Message composition

Volume

Blacklists

Complaints are a main contributing factor to your sending reputation, so minimizing complaints and keeping your content (and frequency) relevant to the individual user should be a goal for every sender.

Content:

Content analysis technology scans every part of an email, including the header, footer, code, HTML markup, images, text color, timestamp, URLs, subject line, text-to-image ratio, language, attachments, and more. For some content filters, there is not one part of the message that the content filter ignores. Other content filters may look at only the structure of an email, or they might simply parse URLs out of the message and then reference them against blacklists.

Spam filters are an integral part of the email ecosystem. Without them, email simply wouldn't work—billions of spam messages would overload the system. Filters are our friends; as users we appreciate when they keep unwanted mail out of our inbox but we're also pleased to get the mail we do want. And filters are the reason that important transactional emails land in our inbox, where we can find them when we need them.

Chapter 4
How Your IP Address and Domain Impact Deliverability

As discussed in Chapter 3, the source of an email is one of the main aspects that mailbox providers consider when filtering messages. The two components that make up an email's source are the IP address and domain.

IP address

An IP address is a number listed in the domain name system that sends mail on behalf of your domain name. Mailbox providers check the reputation of IP addresses sending emails on the behalf of your domains when determining whether or not to place your mail in the inbox.

There are two types of IP addresses that are relevant to marketers:

Dedicated IP address is used by a single sender or company. An IP address that is dedicated to a specific sender means that no other marketer or company is sending email from this IP address.

Shared IP address is used by multiple marketers or companies to deploy email. Because the overall reputation for that IP address is based on all mail deployed from it, the IP address reputation cannot be managed by an individual sender. As a result, all senders are negatively affected if even one sender on the shared IP address is sending spam.

Best practices dictate that most senders should utilize a dedicated IP address in order to maintain full control over the quality of email that is sent across this IP address. (However, there are some exceptions.)

In order to evaluate your IP address reputation, Return Path offers a tool called Sender Score, which operates much like a credit score. The lower your Sender Score, the worse it is for your reputation at that IP address. Each Sender Score is determined by factoring a sender's performance across key reputation metrics important to both mailbox providers and your email recipients. Your Sender Score is an indication of inbox potential, but it's only one of many data points you need to determine how mailbox providers may be filtering your emails.

Understanding sending permanence

Sending permanence relates to the mailing history on of an IP address. Many marketers starting a new email program or changing IP addresses aren't aware of the consequences of sending from a new IP address, so they send to their entire list from day one.

Mailbox providers will restrict the number of inbound emails they will accept from a new IP address (called "throttling") and often filter mail into the junk folder until they monitor consistent, legitimate volume over the IP address. Once consistency is reached, the restriction is either reduced or lifted.

Mailbox providers apply throttling measures for new IP addresses because spammers will often use random IP addresses to send large quantities of email, so achieving consistent traffic over your IP addresses helps to identify you as a legitimate sender.

Following are a few things to keep in mind regarding sending permanence:

Don't run from trouble
You can't escape a poor reputation by moving to a new IP address. Make the appropriate changes to your program to improve your reputation or the issues will resurface on the new IP address.

Don't hop from one IP address to another
Sending from multiple IP addresses isn't always better. Spammers tend to leverage a large pool of IP addresses, hopping from one to another in order to game the system. This technique is known as snowshoeing and puts you at risk for being blacklisted.

Warm up your new IP address
It's important to start slowly with a low send volume, in order to establish an IP address reputation. You can then build up to a greater volume over time.

Maintain consistent send volume
Mailbox providers tend to filter mail when dramatic spikes in volume are observed. Once a positive reputation is achieved on an IP address, strive to maintain consistent volume levels. Senders with inconsistent sending patterns (e.g., seasonal businesses) will need to put some additional strategies in place to address sending permanence.

Domain

A domain name is the registered name on the internet (i.e., companyxyz.com). A domain reputation is the sending reputation for the domain name. This can be the subdomain or the domain, and is usually tied directly to the signing domain used in the authentication protocol DKIM.

Some of the metrics mailbox providers are likely to use when determining domain reputation:

Spam folder placement rate
How many times mail from this domain went into the spam folder due to IP address reputation or content filters

Inbox placement rate
How many times mail from this domain went into the inbox

Complaint rate
How many times a recipient marked a message from this domain as spam

"This is not spam" rate
How many times a recipient went into their junk folder and marked a message from this domain as "not spam"

We'll take a closer look at these and other metrics in Chapter 9. The details of domain authentication are discussed in Chapter 6.

Chapter 5
List Quality and Subscriber Complaints

Ideally, your email list would be populated exclusively with the email addresses of people who are actively engaged with your brand and want to receive your emails. Reality is often very different, but it's important to strive for this ideal because the quality of your email list can have a tremendous impact on your deliverability.

Mailbox providers monitor the addresses to which you are sending and will filter or ultimately block your mail if poor list quality is identified. There are three types of data you want to monitor within your list: unknown users, spam traps, and inactive subscribers. Subscriber complaints are also a strong indicator of poor sending practice, and are an important factor in filtering decisions, as we'll explore below.

Unknown users

An unknown user is a recipient that never existed, has been terminated by the mailbox provider, or was abandoned by the end user. Mailbox providers will return a hard bounce code indicating when email is sent to an unknown user. For example:

```
550 <subscriber@acme.com> User unknown
550 <subscriber@acme.com> Mailbox does not exist
550 <subscriber@acme.com> Invalid recipient
```

All unknown users should be removed from your file immediately via bounce processing (explained in Chapter 6).

An unknown user rate is calculated by dividing the count of email addresses associated with 5xxx unknown user bounce messages by the attempted volume of mail. Keep your unknown use rate below 2% to achieve high inbox placement. Unknown user rates exceeding 10% will likely cause deliverability issues.

Spam traps

Spam traps are email addresses that don't belong to active users and are used to identify both spammers and senders with poor data quality practices. Mailbox providers, filtering companies, and blacklist administrators create and manage spam trap networks to monitor email received at these addresses.

When a mailbox provider sees a sender hitting spam traps, they question the sender's list quality, as spam trap hits are an indication that the sender either 1) acquired the email addresses through questionable means, or 2) is a legitimate entity with poor list hygiene. They then place verdicts on the sender's IP address, domain, or content, which allows their partnering mailbox providers or filtering companies to take action such as placing a temporary (or even permanent) block on the sender's email. The type and age of the spam trap often influences the tolerance a trap operator has, and the severity of verdicts placed on senders who hit spam traps.

There are two types of spam traps:

Recycled spam trap

These addresses once belonged to a real person, but were converted into a spam traps after being abandoned. Recycled traps identify legitimate senders with weak list hygiene and data quality practices.

Pristine spam trap

Also called "honey pots," these addresses were set up solely to capture bad mailers and were never used by a live subscriber. Many spam trap operators will hide their spam trap email addresses on websites, so they are only visible to harvester robots. When senders harvest email addresses from websites, they gather pristine spam traps. Any email sent to these addresses is considered spam.

Following are some recommendations for eliminating both unknown users and spam traps from your email list:

Quarantine new data until you send a welcome message and do not receive a 5xx unknown user bounce. This keeps you from adding bad addresses to your regular campaigns.

Provide easy update options. People often change email addresses and may be willing to update their contact information if you make it easy. Even if you don't have a full preference center, offer change of address and frequency options at the point of unsubscribe.

Consider double opt-in. Marketers who make customers take an action—usually clicking a link—to confirm their subscription generally have smaller lists than they would otherwise, but those lists are much cleaner than non-confirmed lists. They also tend to have lower complaint rates and better inbox placement rates.

Select data sources carefully. Vet third party data sources and perform regular audits on the data they provide. Consider tracking data sources throughout the subscriber lifecycle, to make more informed decisions about third party data sources.

Email your list regularly. In general, the less often you send email, the more likely you are to see high bounce rates. Infrequently emailed lists are also more likely to harbor spam traps as old addresses may have been converted into trap addresses since your last campaign. For more information about optimizing send frequency, check out our recent report, *Frequency Matters*.

Monitor subscriber activity. As a rule of thumb, a subscriber who has been inactive for more than a year and is not responsive to your re-engagement campaigns should be removed from your list. Implement shorter time periods of six months or even 90 days if you mail frequently or send third party advertising. But keep in mind that every sender is different—you should test to determine the strategy that works best for your business.

Run basic list hygiene processes. Regularly clear out role accounts (sales@domain.com), obviously bogus addresses (test@test.com), and errors (jane@gmal.com).

Inactive subscribers

Inactive addresses represent customers on your list file who have not opened, clicked, or taken some kind of action for a significant amount of time. Most marketers have a large number of inactive addresses on their email file. For some, this segment can represent as much as 70-80% of their email file.

Inactive subscribers are undesirable for many reasons. Not only could these addresses be a source of unknown users or spam traps, but they also bring down response rates for the entire program and negatively impact your overall reputation.

To best manage your email program, get a process in place to identify inactive subscribers.

Use campaign performance tracking data to analyze typical email response over time.

Track opens, click, and bounces. Note when opens and clicks drop off and bounces rise. Use that data as a baseline for separating your active and inactive email addresses. After these groups have been identified, reduce the mailing frequency to inactives.

Audit sources of inactive addresses. Review the sources of the inactive email addresses (e.g., online quote, affinity partner, referral, etc.) to determine any behavioral patterns tied to source.

Complaints

One of the main goals of mailbox providers is to protect their users. As such, they place a high degree of importance on their users' feedback and preferences. If email recipients are complaining about your email, mailbox providers will perceive your email as unwanted and will block your mail from the inbox. As a result, complaints are among the most important contributors to a poor sender reputation.

There are three ways a subscriber can register a complaint:

This is junk/spam button: The subscriber hits the junk or spam button (or equivalent) in their email client.

Postmaster complaint: The subscriber sends a message complaining about a sender to the postmaster group at the mailbox provider.

Filter application complaint: The subscriber sends a complaint to a filtering application or a complaint-driven blacklist.

Email recipients complain for many reasons, but tracking down the source of your problem can take some effort.
Here are a few suggestions:

1. Take a look at all of your list acquisition sources so see whether any of them generate a disproportionate number of complaints. Take steps to clean up your list acquisition practices, or remove the bad source(s) altogether. Paid lists, affiliates, and peer-initiated web forms are common culprits.

2. If subscribers don't recognize your brand or remember signing up for your email program, they're likely to complain. A well-executed and timely welcome message can bring subscribers into the fold, educate them about your brand, and reinforce the benefits of your email program.

3. Content that's not relevant or interesting to your subscribers is a target for complaints. Refine your email preference center to get a better idea of the content your subscribers want, and use that information to create highly targeted emails.

4. Make sure your unsubscribe link is prominent and the process is simple. People will often hit the "spam" button if they can't figure out how to unsubscribe.

5. Be aware of complaints by enrolling in all available feedback loops (discussed in Chapter 7). This will ensure that mailbox providers are notifying you of any complaints so that you can remove the subscribers from your list promptly.

Even small variations in complaint rate can have a major impact on your inbox placement. Keep complaint rates below 0.1% for optimal inbox placement. For more information about subscriber complaints and how to manage them, download the *Marketer's Guide to Subscriber Complaints*.

Chapter 6
Authentication and Other Infrastructure Considerations

You can't build a great email program on a weak foundation. You must have a solid foundation (or "infrastructure") comprised of accurate authentication, bounce management, and feedback loop processing if you're going to build a world-class email program.

Authentication

Authentication technology allows the receiver of an email and the mailbox provider to confirm the identity of the sender. If the identity of the sender cannot be authenticated, then mailbox providers may reject the message or put it through additional filters to determine whether it should be delivered.

Without authentication, your chances of being filtered or blocked by major mailbox providers are increased. As a legitimate business, authentication is not optional; it is essential to securing your brand and online reputation. There are the three primary methods of authentication:

SPF (Sender Policy Framework):
SPF is an IP address-based authentication that validates that a message came from a mail server (IP address) that is authorized to send mail for the sending domain. SPF checks are performed on the return-path domain found in the header of your message.

DKIM (DomainKeys Identified Mail):
DKIM provides a method for validating the domain name you send your messages from by using publicly available cryptographic authentication. It signs each message in a way that is difficult to forge, proving that the message came from the indicated sending domain.

DMARC (Domain-based Message Authentication, Reporting, & Conformance):
DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards, and that fraudulent activity appearing to come from legitimate domains is blocked.

DMARC by the Numbers*

35%
Of messages received by large mailbox providers are from domains protected by DMARC

50%
More sending domains publishing DMARC records over the course of 2014

200%
Increase in messages protected by a DMARC "reject" policy over the course of 2014

6x
More sources sending DMARC reports over the course of 2014

Source: *DMARC Intelligence Report*

Authentication is important because it:

Builds your domain reputation. Although a sender's reputation is primarily attributed to the sending IP address, domain reputation is becoming a key factor with mailbox providers. Domain reputation is based on DKIM and DMARC authentication.

Creates a portable reputation. Your domain reputation will move with you regardless of what IP address you're using to deploy mail.

Protects your brand against phishing and spoofing. DKIM and DMARC help protect your brand if spammers try to spoof your domain by allowing spoofed emails to be flagged or blocked by mailbox providers.

Offers you eligibility to sign up for Yahoo feedback loops. Yahoo feedback loops are domain based and require senders sign their messages with DKIM in order to sign up for the program and receive complaint feedback.

Keep in mind, authentication will not solve your deliverability problems. While authentication will make it harder for your domains to be forged, it will not compensate for weak reputation practices.

Bounce management

When a mail server unsuccessfully attempts to send a message to another server, it will typically result in an automated email response called a bounce. Bounces contain a numeric code and a brief description that helps the sender understand why the message was not delivered.

Bounces are generally classified in two categories:

Hard bounce:
A notice that the email message did not go through to the intended recipient because of a permanent failure; for example, email to an invalid address (unknown user), or a rejection due to spam filters. Simply sending the email again later will not result in successful delivery. If the bounce is reputation-related and the sender adjusts practices to improve reputation, resending may get the email delivered. A hard bounce code begins with a 5, such as "<subscriber@example.com> 550 Message rejected."

Soft bounce:
A notice that the email message was sent to an active address but was turned away before being delivered to the intended recipient. Often the problem is due to a temporary issue (like a server outage or full mailbox) or volume (telling the sender to slow down). The email may be successfully delivered if sent again later. A soft bounce code begins with a 4, such as "<subscriber@example.com> 421 Try again later."

Both hard and soft bounces can result in a policy block. Mailbox providers may block your mail due to complaints, lack of throttling, or exhibiting spam-like characteristics. While the addresses causing these blocks do not need to be automatically removed from your file, you should stop mailing to the domains generating these blocks until the reason is identified and you resolve the issue.

Following are some suggestions for bounce management:

Remove hard bounces. True hard bounces (unknown users, bad domains, invalid addresses) should be removed from your list after the first non-reputation related hard bounce.

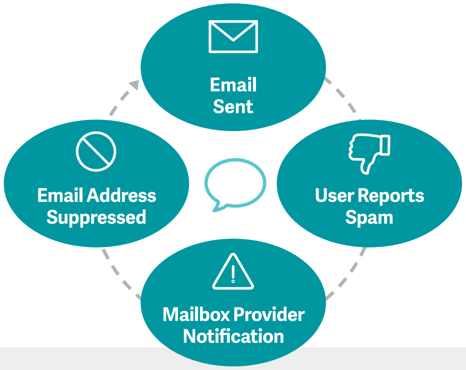
Classify reasons for hard bounces. Create a reporting tool with an alert mechanism to help you classify what the hard bounce rejection reasons are, process the ones that need to be deactivated and keep you up-to-date on why other emails are not getting delivered (policy blocks).

Examine bounce messages. The threshold for removing soft bounces should be set based on your business objectives and mailing frequency. You should also examine the content of bounce messages carefully to determine whether an address should be suppressed permanently.

Monitor soft bounces. Soft bounces should be monitored and the bounce messages reviewed as they can provide valuable information about why a mailbox provider may be blocking or throttling your email.

Feedback loop processing

To help email marketers track complaints, many mailbox providers offer what is called a feedback loop (FBL). When an email recipient reports email as spam, the mailbox provider forwards that email back to the sender. Generally, mailbox providers expect that these transactions will be processed as unsubscribe requests and that the sender will research the nature of the request to reduce complaints.



Following are some suggestions for feedback loop processing:

Collect and suppress complaints. Subscribers who complain should be removed from your email list immediately. Failure to do so could result in additional complaints if the subscriber receives additional email from you.

Monitor complaint rates via the feedback loop data received.

Make adjustments: Analyze this data to determine the cause for complaints and make the appropriate adjustments to your email program. Consider such things as the campaigns, data source, and the age of the data generating complaints.

Chapter 7
How Content Affects Deliverability and Rendering

Back in the early 1990s, mailbox providers were just starting to give out free personal email accounts to anyone who wanted them. Ecommerce was growing, and this represented a new, low-cost opportunity for marketers to advertise their products—but there was little regulation, much less CAN-SPAM laws.

With the surge of promotional email volume, mailbox providers struggled to determine whether a message was in fact legitimate mail or spam. Content filtering was often the first line of defense, checking for known patterns, keywords, blacklisted URLs, and other aspects within the content of the message.

Since then, mailbox providers have greatly advanced their spam filtering technology. Content is still a consideration, but many other factors come into play such as IP address and domain reputation, sending infrastructure, engagement, complaints, and more. In addition, content is a significant factor in individual engagement, which in turn drives filtering.

The filtering process

When a message is received by a remote mail server, it first considers aspects such as reputation, blacklists, and information from the headers received during the SMTP conversation. This allows the receiving software to decide whether to allow, filter, or block the incoming message based on domain or IP address reputation and authentication.

If the receiving server allows the message to move through the next stage, then the full content of the message is received and evaluated. Based on the information within the body of the message and the subject line, it determines whether to mark the message as spam or deliver it to the inbox.

Anti-spam software is constantly learning by gathering information over time from user feedback (retrieving legitimate message from the junk folder or marking messages as spam). So ensuring consistent inbox placement from a content perspective requires regular fieldwork and adaptation for senders.

How to improve your content

It's safe to say there's no silver bullet, because there is a long list of criteria used in determining whether a message should be considered spam. Every single mailbox provider and anti-spam software has its own "secret sauce" when it comes to reading and understanding the content of incoming messages. But there are certainly steps you can take to improve the chances your messages will pass content filtering.

Balance text and imagery. Don't create messages as a single large image, as this is a common spammer technique used in attempt to bypass spam filters. Embedding large images in emails or using a lot of graphics can also slow the email server's ability to process mail. As a result, content spam filters will often flag such emails and stop delivery. Keep in mind also that some mailbox providers turn images off by default, so it's likely images won't be seen anyway. As a rule of thumb, we advise a good balance of text and images. The overall goal is to have enough text in the body of the message so subscribers will understand what is being conveyed whether images are on or off.

Check your HTML. Most emails today are created in HTML, so having a nicely formatted HTML message is a good start. Broken HTML can lead to a poorly rendered message and generate complaints if recipients believe it's a phishing attempt. Make sure your HTML is free of syntax errors and formatting errors.

Test, test, test. Testing message content in a pre-deployment tool such as Return Path's Inbox Preview can help to identify potential spam filter issues before you send. Once you identify content that is being flagged by spam filters, continue testing to isolate what is causing the issues (subject lines, URLs/links, text, and/or images). Content testing can be a time consuming process, but well worth the effort.

Avoid base64. Messages that have a base64 encoded body or subject line are more likely to be flagged as spam by anti-spam software, mainly because this is a known tactic used by spammers to hide the content from anti-spam software.

Fingerprinting

Most senders know that the content of their email is scrutinized for "spammy" content, but it's interesting to understand the methods used to examine content. One well-known method of analyzing content is called "fingerprinting." Some technology providers are known for creating fingerprints of email content. Fingerprinting in and of itself is not a filter, but it is a technology that helps mailbox providers make decisions about email content.

Fingerprints are hashes or checksums of content. These hashes are many times smaller (64 bytes) than the content that they're generated from, which makes them easier to store. Once the fingerprints are created and stored, they can be compared to other fingerprints. The result of the comparison helps filters decide whether or not email is spam by scoring the similarity of fingerprints, meaning if your fingerprint is highly similar to a fingerprint belonging to email that has been confirmed as spam, then your mail will likely be flagged as unwanted mail.

Chapter 8
Understanding Blacklists

Today there are more than 300 publicly available blacklists, ranging from well-known and widely used lists to independent blacklists. But not all blacklists are created equal when it comes to the impact they have on your deliverability. In fact, anyone can start a blacklist and decide what factors will result in being listed.

As a result, mailbox providers and filtering companies have to identify which blacklists will actually help them stop spam from reaching their customers. They will often incorporate a combination of public blacklist data and their own private internal blacklist to create proprietary filtering rules to help determine whether to accept or reject email.

There are two main types of public blacklists: IP address based and domain based.

IP address based:

Real-time Black Lists (RBLs) and Domain Name Server Black Lists (DNSBLs) are lists of IP addresses that can be queried in real-time. Mailbox providers use these to identify whether the IP address of the sending server belongs to a sender that allows other servers to connect and send from their system (open-relays), are known spammers, or allow spammers to use their infrastructure. Some of the more common and widely used RBLs/DNSBLs include:

Return Path Reputation Network Blacklist (RNBL): This RNBL is a real-time list of senders that have been categorized as the "worst of the worst" by the reputation network. It uses a predictive model that analyses more than 600 variables to score IP addresses in real time by incorporating volume, spam trap, and complaint sources.

Sbl.spamhaus.org (SBL): The Spamhaus Block List (SBL) is the most influential Spamhaus blacklist. It is managed by volunteer editors who look for senders that hit their spam trap networks and manually list senders that look abusive. As a trusted blacklist in the industry, an SBL listing can have a very negative impact on your deliverability. Getting delisted from the SBL will require you to develop and execute an action plan to rectify the problem that caused the listing.

Xbl.spamhaus.org (XBL): The Exploits Bot List (XBL) includes the IP addresses of servers that are known to have security problems such as open proxies or sending executable viruses. Most IP addresses are listed as a result of sending spam or viruses to Spamhaus spam traps. If listed, your system is likely compromised and you need to take action to secure your system. The XBL incorporates the CBL blacklist as well as other lists of spam sources related to compromised systems.

Cbl.abuseat.org (CBL): The Spamhaus Composite Blocking List (CBL) only lists IPs that exhibit behavior indicating it is an open proxy being used for sending spam or a virus. The CBL offers an easy self-removal option here.

SpamCop (SCBL): The SCBL includes a list of IP addresses that have sent reported spam to SpamCop users. The length of listing varies depending on how many spam reports are received. Delisting occurs automatically 24 hours after spam reports stop.

Psbl.surriel.com: The Passive Spam Block List (PSBL) is a list of IP addresses that have sent email to their spam traps and the IP address is not a known mail server. They do encourage whitelisting to stay off their list.

Ubl.unsubscore.com: Lashback's UBL lists IP addresses of senders that are sending email to addresses that have been harvested from suppression lists.

Invaluement: The Invaluement Anti-Spam DNSBL consists of three separate lists: ivmSIP which includes IP addresses that only send spam, imvSIP/24 is similar to the imvSIP except it will list an entire block of IPs and ivmURI which is their domain based blacklist. While other blacklists use spam traps to identify IPs for listing, Invaluement targets spam sent to real users as well as snowshoe spam.

Domain Based:

URI Real-time Blacklists (URI DNSBL) are lists of domain names that appear within the email body. This blacklist will look for the URLs within the body of the email to see if it contains a domain that has been identified as a source of spam. These blacklists will not only look at the initial link, but those it redirects to as well to see if they contain the spammy domains. The most commonly used URI DNSBLs include:

Dbl.spamhaus.org: The Spamhaus DBL is a real-time blacklist that includes domains found in spam messages. Maintained by both an automated system and global team members, listings automatically expire when the domain no longer meets the proprietary criteria and no longer appear in spam email.

URIBL: The URIBL is a list of domains that have been identified as being used in spam email. While they have several public lists, the most common list that can result in delivery issues is the black.uribl.com which has a goal of zero false positives. The list updates frequently as new data is received, so delisting can occur automatically. The domain owner may also request removal once registered with the uribl.

SURBL: SURBL is a list of website domains that have appeared in unsolicited messages. The domain owner may request removal by conducting an initial lookup and following removal instructions here.

If you find yourself listed on a blacklist, take time to evaluate the impact of the list overall as well as the specific impact to you as a sender. If you determine that getting delisted is important, keep in mind that you must resolve the problem that caused you to be blacklisted before submitting a delisting request—even if the blacklists has a self-removal site. Failure to do so will result in your being listed again, and over time your requests can be rejected. Get to the root cause of the listing, fix the issue, and avoid the vicious cycle.

Return Path's *Ultimate Guide to Blacklists* infographic provides additional information about the blacklist landscape, their impact, and how to evaluate the potential risk to your email program.

Chapter 9

Subscriber Engagement and Spam Filtering

Every marketer wants an engaged subscriber base—people who like receiving your emails, open them regularly, and interact with the content. Engagement is also a key factor in filtering, but how do mailbox providers evaluate subscriber engagement?

It turns out each provider has its own methods for measuring engagement. Some are more sophisticated than others but all evaluate subscriber engagement to make inbox placement decisions. Microsoft, AOL, Gmail, and Yahoo lead the industry in their use of engagement metrics to determine filtering.

Mailbox providers identify patterns in engagement with mail from specific IP addresses or senders, and assess the significance of those patterns by asking questions like:

Are messages being sent to real people? Mailbox providers focus on the sending IP address' ratio of messages sent to real accounts versus test accounts.

Are those recipients active? Mailbox providers look for indicators like frequent logins, reading email, sending email, and reporting spam.

Are those recipients trustworthy? Mailbox providers look at how long customers have held accounts, how frequently they're active, and the consistency of their spam/no-spam reporting patterns. These signals are then used to assign relative weights to marketers' engagement.

Mailbox providers look at hundreds of factors to determine whether or not an email is wanted. But for engagement-based spam filtering, the most important metrics are:

Messages read
A positive indicator that the individual wants to receive your emails

Messages replied to
A positive indicator that the message is likely personal in nature, and desired

Messages marked as "not spam"
A very strong positive signal that mailbox providers use to train their spam filters

Messages marked as spam
A very strong negative signal that your email is unwanted and does not belong in the inbox

Messages moved to other folders
An indication that the recipient not only wants your email, but also wants to organize it and access it later

Senders/domains added to address book
A positive signal indicating that future messages should be delivered to the inbox

Messages forwarded
A positive indicator that the recipient values the message and thinks that others should see it, too

Click-through rate and engagement-based filtering

We know that mailbox providers don't include click activity in their engagement algorithms. If that's true, then why have so many deliverability experts advised email marketers to look at clicks?

The advice to look at click-through rates to get a handle on engagement-based spam filtering is primarily due to the fact that marketers often don't have access to the same metrics as the mailbox providers. Most marketers today can easily see messages opened/read and messages marked as spam in their own email reports, but little else.

This means that marketers are flying blind when it comes to other important metrics like:

How many of their messages were marked as "not spam"

How many emails were deleted without being read

How many emails were forwarded

How many emails were moved to a different folder

How many subscribers added them to their personal address book

Until recently, these metrics weren't available to anyone. As a result, marketers and deliverability consultants had to look at the closest proxy: opens, clicks, and conversions. The metrics a marketer would use to determine whether they had issues with engagement-based spam filtering were determined by how much data they were collecting.

Looking at data beyond email analytics, like past purchases, downloads, and website activity will always be a stronger gauge of engagement filtering issues than simple opens and clicks.

Following are some best practices for ensuring that every subscriber receives the right message, at the right time:

Build relationships. To get subscribers engaged, senders need to build solid relationships from the beginning. Set clear expectations, send a welcome message, and then follow through with what you've promised.

Deliver messages designed to engage. Capture attention with compelling subject lines, content that renders beautifully on any device, and offers that align with subscribers' interersts.

Send email when subscribers are in their inbox. Know your subscribers' email patterns and send mail when they're most likely to see it and take action.

Consider the "real world." Keep in mind that a subscriber's interests can change (e.g., parents won't always have a baby or toddler), and develop a strategy that takes the subscriber's lifecycle into account.

Re-engage inactive customers. Develop a strategy to bring customers back into the fold and get them engaged with your program.

Monitor engagement metrics. Engagement-based metrics like "deleted unread" and "marked as not spam" are available today through subscriber panel data providers (like Return Path). These provide a much better way to measure personalized inbox filtering decisions and determine whether engagement filtering is actually a problem.

Re-engaging inactive subscribers

Inactive subscribers can pose a liability to the health of your email program. But unfortunately, every email list includes customers who are not actively engaged.

Re-engagement campaigns provide an opportunity for senders to recapture the attention of inactive subscribers and protect the health of their email list. Keep in mind that because customers have different reasons for becoming inactive, you may need a number of re-engagement tools in your arsenal.

These may include:

- Special offers
- Access to exclusive content
- Promotion of new content, videos, or "how-to" tips
- Invitations to opt-down or opt-out
- Opportunities to update email preferences

If subscribers have reached an inactive state and do not re-engage after several attempts, they should be removed from your list. Though there is a small chance they may respond at some point, keeping them on your list and sending additional mail increases the likelihood of unknown users and spam traps.

Chapter 10
Deliverability Metrics and Measurement

Marketers recognize the importance of measuring every aspect of their email program, to prove its effectiveness and demonstrate its impact on the bottom line. But which metrics are the most important?

Metrics are often divided into chronological categories, according to where they occur along the buyer's journey. We prefer to classify metrics differently, based on what they actually tell you about your email program. Accordingly, we've divided 16 of the important metrics into three categories: Awareness, Clarity, and Connection.

Metrics to enhance your awareness of email performance

We discuss the most basic category of metrics in terms of "Awareness," because they offer high-level visibility into the health of your email program. These metrics provide simple insights into what's happening within your email program—and may tip you off to potential problems—but they don't go deep enough to provide any truly actionable insights.

Delivery rate
Calculated by dividing the volume of emails delivered by the volume of emails sent. Note: "delivered" doesn't necessarily mean your email hit the inbox—just that it wasn't bounced or rejected.

Bounce rate
Bounced email is the opposite of delivered email. These are the messages that fail to get delivered for any reason.

Rejected rate
Rejected email is a subset of bounced email, and includes only those messages that fail to get delivered due to reputation issues (e.g., complaints, spam traps, blacklisting).

Inbox placement rate*
Inbox placement rate measures the percentage of sent email that actually lands in the subscribers' inbox—a far more accurate measure than delivery rate.

Open rate
Calculated by dividing the number of emails opened by the number of emails delivered. This metric is actually less useful than you'd think, because an email will not register as "opened" unless images are displayed in the message—either through settings or active loading.

Click-through rate
Calculated by dividing clicks by the volume of email delivered. This metric is commonly used to measure email engagement, but it is actually far less useful than click-to-open rate, discussed later.

** Available only from Return Path*

Metrics that provide clarity around email performance

Taking things a step further, we have "Clarity" metrics. These measures take the analysis of your email program to a deeper level and provide more sophisticated insights into deliverability and engagement. Some provide a more granular view of "Awareness" metrics, while others can help you uncover the "why" behind email performance issues.

Hard bounce

Hard bounces are messages that are permanently rejected, typically due to issues with list quality (e.g., invalid email addresses or domains).

Soft bounce

Soft bounced are messages that are temporarily rejected, typically due to issues with the recipient's mailbox or server (e.g., mailbox too full or server down).

Read rate*

Read rate is similar to open rate, but it is far more accurate because it accounts for all emails viewed, regardless of image rendering.

Complaint rate

Calculated by dividing the number of spam complaints by the number of emails delivered. Complaints are a strong indicator of negative engagement and this metric is useful for identifying patterns and sources of complaints, but may be distorted by deliverability issues.

Deleted before reading rate*

Measures how often a recipient deletes email without reading it. This metric provides powerful insight into the difference between subscribers who do not want to read your email and those who may just check their email infrequently.

Unsubscribe rate

Calculated by dividing the number of unsubscribes by the number of emails delivered. Be cautious of using this metric in isolation, as a declining unsubscribe rate can result from various things such as improving engagement or a decreasing inbox placement rate—two very different situations.

Metrics to evaluate subscriber connection

The most sophisticated—and often most valuable—category of metrics relates to "Connection." These metrics provide the truest measure of whether subscribers are engaged with your brand, as well as the depth of their engagement. Properly interpreted, Connection metrics can help you evaluate specific aspects of your email program, like the effectiveness of your content and design.

Click to open rate

Measured by calculating the ratio of total clicks to total opens. Click to open is the best and most accurate of the click-based metrics, and provides valuable insight into the effectiveness of your email content and design.

"This is not spam" rate*

Measures how frequently recipients click on the "This is not spam" button after an email is delivered to the spam folder. This metric is a powerful indicator of subscriber engagement.

Forwarded rate*

Measures how frequently subscribers forward your email on to others. This metric is useful to gauge the virality of your content, and a high forwarded rate indicates strong subscriber engagement.

Conversion rate

Calculated by dividing the number of conversions by the number of visits. Although a strong indicator of subscriber engagement, this metric typically speaks more to the quality of landing page or website content than email content.

** Available only from Return Path*

Getting more out of your metrics

For additional insights, consider subsets of these metrics, as well as the relationships that exist between certain metrics.

Total vs. unique: Certain metrics like opens and clicks can be divided into "total" and "unique," which eliminates duplicate actions by the same subscriber, to provide a more accurate measure of activity. The ratio of total opens/clicks to unique opens/clicks can also provide useful insights into engagement levels.

Ratio of unsubscribes to complaints: If complaints are higher than unsubscribes, this could indicate potential issues with your opt-out process.

"Positive" clicks vs. "negative" clicks: Total clicks can be misleading if a high percentage are for non-offer links such as "Terms & Conditions."

Disaffection index: The aggregate of all churn metrics: bounces, unsubscribe requests, and spam complaints.

Sign-up vs. churn: If subscribers are being lost from the program faster than they are being added, there may be fundamental issues with your email content, or with the expectations you're setting at sign-up.

For more information about using metrics to troubleshoot problems with your email program, check out Return Path's *Guide to Email Marketing Metrics*.

Email benchmarks

Viewing campaign results in a vacuum provides little value. Benchmarking individual campaigns against other campaigns and benchmarking your overall email program over a specific period of time (e.g., year-over-year, quarter-over-quarter), provides insights into the overall health of the email program.

The use of industry benchmarks can also help provide a baseline and can also highlight potential areas of opportunity. However, please note that any benchmark data should only be used as a guideline because specific aspects of each company's email program drive different results. For instance, individual types of campaigns (transactional vs. acquisition vs. retention) have different average open and click rates.

Chapter 11
Debunking Common Deliverability Myths

Myth #1: My "delivered" rate shows how many emails were delivered into the inbox.

Why this is fantasy:
Delivered rate is one of the most widely used measurements in email marketing, but this metric is highly deceptive and completely misunderstood. The delivered rate doesn't actually measure how many of the emails landed in the inbox ; it simply tells you how much of your mail avoided being bounced or rejected.

The plain truth:
Rather than aiming for a 99% delivered rate, aim for a higher inbox placement rate, and get as much mail delivered and seen to as many subscribers as possible. Maintain good list hygiene, respect the expectations of your subscribers, and send compelling messages at the optimal time to stand out in the inbox.

Myth #2: It's my mailbox provider's job to fix my deliverability issues.

Why this is fantasy:
Sure, your mailbox provider might be responsible for some deliverability issues if the send infrastructure isn't set up properly, or they assigned you a shared IP address with a poor reputation. These scenarios are usually the exception, and not the rule. As a sender, you are in charge of your own email deliverability and reputation. Your reputation is determined by the quality of your lists, complaints, message quality, and subscriber engagement, all of which you control. When mailbox providers are concerned about your deliverability, they're looking to protect their network, business, and customers by only allowing senders with a good reputation to send from their systems.

The plain truth:
Unless you address the root cause of your poor reputation, no mailbox provider can get you delivered to the inbox.

Myth #3: I don’t need to worry about inbox placement if I have a high Sender Score.

Why this is fantasy:

Sender Score indicates the trustworthiness of an email sender’s IP address to a mailbox provider or filtering company. It tells mailbox providers the probability that their email users will think your email is spam. Sender Score is more of an indication of your inbox potential than anything else. At the end of the day, it’s still only one of many data points you need to determine how mailbox providers may be filtering, blocking, or bulking your emails instead of delivering them to the inbox.

The plain truth:

Your Sender Score isn’t the same as your inbox placement rate. Instead, think of a low Sender Score as a higher likelihood that email sent from your IP address will be classified as spam. A high Sender Score is a lot like TSA Pre-Check at the airport. You may be able to keep your shoes and belt on, but you still have to have to go through the metal detectors

Myth #4: I have a low complaint rate, so my mail should be delivered to the inbox.

Why this is fantasy:

Complaint rates are calculated based on total number of complaints and total messages delivered to the inbox. If your mail is getting delivered to the spam folder, you could potentially have a low complaint rate, because it’s not possible to mark a message as spam if it’s in the spam folder. If you’re getting sent to spam, it’s the “this is not spam” rate you need to be consider. Some filters and mailbox providers even go a step further and only count complaints from active, trusted subscribers—meaning that all those inactive email addresses on your file who never complain won’t be counted in the denominator. That means your complaint rate is probably much higher at the mailbox providers and filters than you think it is.

The plain truth:

Complaints are a factor, but not the only factor that goes into understanding your deliverability. As the email deliverability landscape becomes more complex, you’ll need to get a better handle on the metrics that can also positively affect your inbox placement rates, like the “this is not spam” rate.

Myth #5: Words like "free" or symbols like the exclamation point (!) should be avoided because they trigger spam filters.

Why this is fantasy:
Spam filtering systems rely largely on your sending reputation when making inbox and spam folder placement decisions. Content plays only a small role in the filtering decision for senders today, because content spam filters experience too many false negatives, aren't reliable, and are easy for spammers to work around. If you're unsure whether your content is triggering spam filters, use a tool like Inbox Preview to test against the major spam filters that will flag certain keywords, URLs, or HTML issues in your content. After you've fixed the issues that have been flagged, send a pre-deployment test to our deliverability monitoring product, Inbox Monitor, to see whether there are any filtering problems you need to be worried about.

The plain truth:
If you have a good reputation, more often than not your reputation will override any content filter. But that doesn't mean content isn't important. If you're sending third party content or templates used by others, your content might have a bad reputation by association. So while content can influence deliverability, filtering isn't necessarily a result of the content itself.

A Better Way to Use Data

We help the world's leading companies promote and protect their brands.

Email Optimization

The right message, at the right time, to the right inbox means better relationships, greater reach and increased revenue. Email Optimization enables enhanced insights for better deliverability and more meaningful engagements.

Email Fraud Protection

The cost of a cyber attack goes beyond dollars and cents, it damages the integrity of a brand. Email Fraud Protection uses advanced fraud profiling data to respond to, and prevent, cyber attacks with greater speed.

Consumer Insight

The inbox provides a unique real-time view of consumer behavior - from brand affinity to detailed purchase records. Consumer Insight provides in-depth data across millions of global consumers enabling smarter decisions and better business results.

Return Path
FROM VALIDITY

USA (Corporate Headquarters)
rpinfo@returnpath.com

Australia
rpinfo-australia@returnpath.com

Brazil
rpinfo-brazil@returnpath.com

Canada
rpinfo-canada@returnpath.com

France
rpinfo-france@returnpath.com

Germany
rpinfo-germany@returnpath.com

United Kingdom
rpinfo-uk@returnpath.com

returnpath.com

validity

Businesses run better and grow faster with trustworthy data. Tens of thousands of organizations rely on Validity solutions – including DemandTools, BriteVerify, Trust Assessments, Return Path and GridBuddy – to target, contact, engage, and retain customers effectively. Marketing, sales, and customer success teams worldwide trust Validity solutions to help them create smarter campaigns, generate leads, drive response, and increase revenue. For more information visit validity.com and connect with us on LinkedIn and Twitter.

Boston – Corporate Headquarters
200 Clarendon St, 22nd Floor
Boston, MA 02116

Tampa – Principal Office
4010 Boy Scout Blvd, Suite 1100
Tampa, FL 33607

London – Validity International Limited
The Charter Building
Uxbridge, UB8 1JG

validity.com
US: 1-800-961-8205
UK: +44 (0) 118 403 2020
sales@validity.com

Return Path FROM VALIDITY · BriteVerify FROM VALIDITY · DemandTools · Trust Assessments · GridBuddy