



Best Practice Guide: Improve Your Chances for Success

Our goal is to help create world class senders. These best practices will ensure success for the world's best email marketers. Here you will learn how to minimize complaint rates, eliminate spam traps, reduce unknown users and ensure your unsubscribe functionality is compliant.

These elements are the core components of Return Path Certification. By checking your program against these guidelines, you can greatly increase your chances of being accepted to the program as a Certified sender. And if you need hands-on-expertise, Return Path has a whole team of experts dedicated to the art of following best practices for improved deliverability and higher response.

1. COMPLAINTS (“Report as Spam”)

How Subscribers Complain About Email

Complaints occur when subscribers complain about your email. There are several ways a subscriber can lodge a complaint about your email. These are:

1. the subscriber hits the ‘report spam’ button (or equivalent) in their email application;
2. the subscriber sends a message complaining about a sender to the postmaster group at the ISP,
3. the subscriber sends a complaint to a filtering application (like Cloudmark's Spam Net) or a complaint-driven blacklist like Spam Cop.
4. the email was voted as “Junk” during a Windows Live Sender Reputation Data poll.

How to Minimize Complaint Rates

Return Path has the following recommendations for reducing complaints and complaint rates:

1. Find out if Subscribers Are Complaining

More than likely, some subscribers are complaining about your mail. It happens to everyone. However, you need to know how serious the complaints are and if they are hurting your email reputation. You can gain access to complaint data by signing up for feedback loops at many of the ISPs. When subscribers lodge a complaint, that





information is captured into a database and made available to you so you can proactively remove complainers from your file and amend your practices accordingly.

Each ISP has a different threshold for acceptable complaint rates. Therefore, it is imperative that you monitor your complaint rates for each ISP using tools like Return Path's Reputation Monitor.

2. Find out why subscribers are complaining.

Does your email program meet subscriber expectations? Examine the subscriber experience. Look specifically for areas where the expectation you set for the subscriber is not played out in the on-going communication with the subscriber. Where you find areas that do not live up to the expectation you've set or where expectations are not clearly set, change them. Pay special attention to the following:

- **Do they know the email is coming from you?**
Make sure you set clear expectations by aligning your Consent and Disclosure statements with your privacy policy and permission practices at the point of sign up. For example, if you are sending third-party offers or simply asking people to sign up for your email program, make sure your subscribers give their explicit consent, and make certain that all email is clearly labeled as coming from you. Sometimes it can be a simple case of mistaken identity.
- **Are you delivering something different than you promised?**
If subscribers aren't interested in your email then they may complain about it. Make sure you are setting the right expectations when they sign up. And remember, subscriber interests can change over time. Offer a preference center. Providing subscribers with choices can help reduce your complaint rate. Make it easy for them to choose the email they want to receive and when. By doing so, you will have an active and engaged subscriber list that complains a lot less about your email.
- **Can subscribers easily remove themselves from your list?**
Make sure your unsubscribe process is clear, conspicuous, and functional. Don't make it hard for them to unsubscribe because you want to prevent them from leaving. If you do, the only alternative is to lodge a complaint by reporting your email as spam. Combat this problem by placing unsubscribe instructions in an area where users are most likely to see it. Allow users to unsubscribe by offering a "one-click" mechanism and provide multiple methods to unsubscribe (like a link to a simple web form or replying with "unsubscribe" in the subject line). Also make sure your email is CAN-SPAM compliant.





- **Are you sending too much email?**

Changing your frequency can cause a spike in complaints. If you suddenly start to send more mail than you originally promised, alert your users so they can opt-out or opt-down from your email program instead of reporting your email as spam.

- **Is your list clean?**

Make sure your data sources are good and reliable. This can be bolstered by your permission practices. For example, validating data at sign up and using double-opt coupled with a welcome message can go a long way to ensuring the data enters your system clean. If you obtain your data from a third party, make sure you vet the partner and perform regular audits.

Once the data is in your system, perform regular maintenance on it. Sending to unknown users and bad email addresses can cause your reputation metrics to nose dive. Take a look at the age of your subscriber email addresses on your list and make sure you are only mailing to active users. By maintaining a clean list, you can also avoid spam traps. (More on spam traps later.)

3. Analyze the Data Regularly

Perform a detailed quantitative analysis of your mailing program to determine where there is a disproportionate amount of complaints generated. When analyzing the data, look for high rates associated with a data source, activity, response rates, customer segments, and content or campaigns. Where you find areas of high complaints, take the appropriate action to either remove the records permanently from your database or eliminate a poor data partner.

Once corrected, complaint rates should decrease over time. Continue to monitor volume and rate of complaints from ISP Feedback Loops and performance tools, such as those offered by Return Path, to ensure continued compliance.





2. SPAM TRAPS

What is a Spam Trap?

Spam traps are a common technique used by receivers, ISPs and filtering companies to identify senders with poor data collection practices. Spam trap addresses are addresses that have been established for the sole reason of catching illegitimate email.

There are two categories or types of spam traps. The first type is a new email account that has never before been used by any user. These accounts do not and will not subscribe to any email communication or are used to communicate in any way. The second type of spam trap is email addresses that were once active, valid users, and have been expired for a significant period of time. These addresses are reactivated and used similarly to new spam traps. They will not subscribe to any email communication or communicate in any way.

It is important to note with the second type of spam trap that senders employing solid bounce management procedures should have deactivated any old addresses reported by the ISP as an unknown user. If a sender continues to send to an address that is so old that it was deactivated and then reactivated as a spam trap, it can be indicative of poor data management as well.

How to Resolve Spam Traps

Maintaining an accurate subscriber database is a cornerstone of email best practices, and receivers have a low tolerance level for senders who mail to their spam trap addresses. Here's what you can do to avoid and resolve them.

1. Regularly Monitor Your Data

Regularly monitor data that provides feedback about your spam trap activity. At a minimum, you should be monitoring the following sources to track your rate of hitting spam traps:

- **Spam Cop listings.** Immediately research them to determine if they are a result of spam trap hits
- **Public DNSBLs** that are indicative of hitting spam traps (e.g. <http://www.blacklistalert.org/>)
- **Aged addresses** that never open or click within your email messages





2. Review your Data Collection and Maintenance Practices

Review your data collection, third party data sourcing, bounce management, and data maintenance practices to identify areas that might allow the collection of spam trap addresses, or that permit the retention of aged and inactive records on your database.

If you are unable to identify problem areas with your data collection, data partners, or data maintenance, you may need to localize the spam trap problem through a process of segmentation of data, and either reconfirming or deleting high risk segments.

Also, if you employ confirmed opt-in procedures, where you send an email confirmation to any email address collected, you may send those confirmations from a separate IP address than where you send the regular email. If someone is signing up spam traps, or potentially mistyping their email address, your confirmation email will be sent to that address and it will count against your IP. Sending confirmations is a best practice, but it comes with this risk, so send them from a separate IP address.

Once you have identified and corrected the problem areas in your mailing program and practices, your rate of mailing to spam traps should decrease over time. Continue to monitor volume and rate of spam trap hits from ISP and performance tools and public blacklists to ensure continued compliance.

Sound like a lot of work? Return Path's deliverability monitoring tools can help monitor spam traps on an ongoing basis, providing you with a singular source to refer to and an account representative to help analyze the data.

3. Unknown Users

How to Avoid Emailing the Dead

Certified senders must use email address list maintenance systems which reliably receive and process bounces and other system replies from receiving networks. Permanent delivery errors from messages sent from Certified IP addresses must be processed by removing the recipient's email address and should not exceed 10% of all messages sent from Certified level IP addresses.

Resolving your unknown user problem is an easy process. You should remove addresses that have a 550 5.1.1 entry in your mailing logs prior to sending your next campaign.





4. Unsubscribe Functionality

Don't Hold Subscribers Hostage

Providing subscribers with the ability to unsubscribe from receiving your mail, and maintaining a process that consistently works and processes requests in a timely manner is a cornerstone of email best practices. And it's required by law via the CAN-SPAM Act. Other than it being illegal, if your unsubscribe process isn't consistently available or is difficult to use, you run the risk of subscribers hitting the "report spam" button just to get off your list.

How to Improve Your Unsubscribe Functionality

1. Review Your Unsubscribe Process

Conduct a detailed review of your current unsubscribe practices. This entails reviewing the actual process that subscribers use to be removed from your list, as well as, reviewing the internal processing of the request that results in the removal of the address from additional mailings.

2. Make Sure Your Unsubscribe Process Works

Our data provider, [Lashback](#) is a company that specializes in monitoring unsubscribe functionality and identifying specific points where the process is not reflective of best practices. Once you have identified and corrected the problem areas in your mailing program and practices, you should see improvements in your ability to efficiently unsubscribe recipients over time. Continue to monitor your unsubscribe processes to ensure that it is easy to use, nearly always available to subscribers, and that requests are processed in a timely manner.