



GET MORE INFO

rpinfo@returnpath.net

1-866-362-4577

Certification Evaluation Kit

Introduction

Welcome, marketers and senders. You are now on the path to experiencing ultra-high delivery rates for your email program. Once you are accepted to the program, you can experience preferential treatment at over 2 billion inboxes worldwide, plus gain added privileges which for many of our customers lead to increased response rates. Return Path Certification works because we all have the same goal. Senders, receivers and consumers all want permission-based email to reach its destination. Certification provides ISPs with a whitelist of trusted senders who meet high program standards, so ISPs can let their mail through with confidence.






Certified senders get higher delivery rates—and that means higher response rates. It's a winning combination that helps make the email channel work better for everyone. So cheers to you for wanting to become the best sender you can be. Let's get you started.

About This Kit

The Return Path Certification evaluation kit contains all the information you will need to ensure you are ready to apply for the program. The standards are high, but the benefits are real. And while this program isn't for everyone, you can certainly elevate your status to receivers if you meet the requirements and maintain the standards of the program.

How to Use this Kit

Use the icons as a guide for completing your application and learning about why and how the program works. Scattered throughout are helpful tips, answers to the most common questions and key definitions.

-  Helpful tips tell you exactly what you need to know for your application.
-  You've got questions. We've got answers. Simply look for them.
-  Definitions to some common terminologies are in the appendix. When you see this icon, flip to the back to get more information.
-  See what clients have said about the program.
-  Stop! Read the information carefully.

Contents

Program Overview	3
What is Return Path Certification?	3
Two Levels of Trust That Help Get Your Delivered	3
Supported Domains	4
Pricing & Fees	5
Certification Pre-Application Checklist	6
Minimum Standards & Requirements	8
How to become a Safe sender	8
How to become a Certified sender	14
Best Practice Guide: Improve Your Chances for Success	16
APPENDIX	20

Program Overview

What is Return Path Certification?

Largest coverage. Bigger benefits. Better results.

Return Path Certification is an exclusive whitelisting program with deep corporate and consumer market coverage. With Return Path Certification, your company can increase delivery rates at more than 2 billion email inboxes worldwide including Yahoo!, Hotmail, and hundreds of other ISPs and spam filter solutions.

Return Path Certification is uniquely designed to help legitimate senders achieve maximum inbox delivery. Our service is built on a network of trust between senders and receivers that provides senders privileged access to the largest, broadest and most respected whitelist in the email universe. Receivers value our whitelist because it provides them with an easier way to separate the good senders from the spammers. As a result, this network of trust is founded on one common goal – to make sure consumers get exactly what they want in their inbox – and based on a firm belief that good marketers should be rewarded for following the best practices that make this channel safe for email.

Two Levels of Trust That Help Get Your Delivered

It's all about trust and partnership.

Return Path Certification offers two levels of trust: Safe and Certified. Your level is determined by your business practices and your reputation performance metrics. The better you perform the more benefits you receive as a world class sender.

Level 1: Safe sender

Leading ISPs and filtering companies rely on our certification program to identify legitimate and reputable businesses. This means our Safe senders experience improved inbox delivery to over 300 million inboxes worldwide. To become a Safe sender, you must meet the Minimum Standards and Requirements of the program ([see page 8](#)). These qualitative requirements address areas of email infrastructure, information security, consent and disclosure, business model and list hygiene.

Level 2: Certified sender

Participating Senders with superior sending reputations may qualify for an upgrade to the Certified level. Certified senders are recognized by ISPs as the “best of the best” in the email universe and therefore, have privileged access to Return Path’s performance-based whitelist used by over 2 billion inboxes worldwide.

Upgrade Your Status

How to Go From Being a Good Sender to Being a Great One!

To be upgraded to Certified, your email must meet superior performance standards and boast a strong reputation. We look at several factors to determine your eligibility for Certified. ([see page 14](#)) Your IPs can be upgraded at any time, and the best thing is that upgrades based on performance happen automatically. The more you follow and comply with the best practices of the program, the more benefits you can reap from the program for each of your IPs.*

Work that is always in progress.

Once you’ve been upgraded to Certified, you want to stay there. Therefore, it is important that you continue following the best practices that made you eligible for Certified in the first place. If for some reason your performance metrics fall short, your IPs will be suspended from Certified, but they will remain on the Safe level until your IPs once again comply with the Certified standards. You will receive notifications whenever this happens so you can take immediate action to regain Certified status.

** Applies to full licenses only.*



If you have questions or would like to hear how Return Path can help, please call 1-866-362-4577, or email rpinfo@returnpath.net. © 2012 Return Path, Inc. www.returnpath.net v032112

Maintain the minimum program standards.

Return Path Certification works because of the strong network of trust that is built between senders and receivers so it is important to note that violations of the Minimum Standards and Requirements may result in suspension of the IP address from the certification program. Severe violations will be investigated on a case by case basis. Excessive and or egregious violations may result in the removal of all IP addresses from the program.

Supported Domains

Hundreds of domains are within your reach.

How many mailboxes do we cover? A lot! Hundreds of domains equal millions (even billions of mailboxes). Safe senders get improved delivery to 300 million inboxes. Certified senders receive improved delivery to over 2 billion inboxes.

For the full list of ISPs, spam filters and other receiving entities go to:

<http://www.returnpath.net/commercialsender/certification/footprint/>

Pricing & Fees

Return Path’s Certification program provides premium access to 2 billion email inboxes worldwide. For senders, there are two pricing components:

Application Fee: To be considered for the program applicants must submit a non-refundable application fee along with the completed application. Our Certification Analyst team evaluates your email program for acceptance and will provide you a comprehensive review of your email program upon completion.

Annual License Fee: Applicants who are accepted to the program must pay an annual license fee which is determined by the volume of email you send per month. The annual license fee covers the day to day management of the service and improvements to the program.

Pricing is based on your monthly email volume.				
Sender Class		Monthly email volume	Application Fee (USD)	Annual License Fee (USD)
Non-Profit*		Up to 250,000	\$ 200	Free
Commercial	Tier 1	Up to 50,000	\$ 200	\$ 440/year
	Tier 2	Up to 250,000	\$ 500	\$ 1,375/year
	Tier 3	Up to 1MM	\$ 650	\$ 2,750/year
	Tier 4	Up to 5MM	\$ 1,000	\$ 9,350/year
	Tier 5	Up to 10MM	\$ 1,000	\$16,500/year
	Tier 6	Up to 20MM	\$ 1,250	\$27,500/year
	Tier 7	Up to 50MM	\$ 2,500	\$55,000/year
	Tier 8	Up to 100MM	\$ 3,500	\$82,500/year
	Tier 9	100MM +	\$ 5,000	Custom Quote

*Non-Profit class is only available for qualified organizations with monthly email volume of 250,000 messages or less. For non-profits above this volume level, the organization is treated as commercial.



How will I know if I am accepted to the program?

Once you submit your application, the review of your email program usually takes 2-6 weeks. Our Certification Analyst team will work with you during this process and will ultimately notify you of our decision via email. Throughout, you will receive occasional updates on the status of your application.

If you are accepted, we will add your IP addresses to the Safe level or upgrade you to Certified level if and when you qualify. If you are not eligible for the Return Path Certification Program, we will highlight best practices you can improve and provide you with specific recommendations on how to qualify. Once you have made the changes to your program you can re-apply and submit a new application fee.

Certification Pre-Application Checklist

Use this handy checklist to make sure you are ready to apply. Plus, we’ve provided some helpful tips to make it easier for you to qualify. If you are unsure of any item, consult the FAQ/definitions on page 20 and/or work with your email or network administrator to get the required information.

Most questions on the application can be answered with a simple “yes” or “no” response, but we’ve provided some tips on where and how to find out if you comply with the standards. Once you have all of the information handy, it should only take about 10 minutes to complete the online application. If you have questions about any of the items in the checklist, refer to Standards and Requirements section on page 8z.

About Your Infrastructure

The Certification program certifies IP addresses. These questions apply to all of the IP addresses you want included for evaluation and acceptance into the program

Infrastructure Standards	Application Tips
Your email is sent over dedicated IP address(es), and you are the only sender that uses them	⊘ You must be mailing off of a dedicated IP in order to be eligible for certification. You will need to list ALL of the IP addresses you want certified on the application as well as all of your mailing domains.
The IP address(es) have at least 90 days of mailing history	⊘ If you have not been mailing for at least 90 days, wait until you reach the 90 day threshold before applying.
You have a fully qualified rDNS record including a PTR record with a corresponding A record that points back to the original IP	📄 You can test your record at this unaffiliated site: http://www.dnsstuff.com/
You have a Sender ID compliant SPF record published for all from and return-path sending domains associated with this IP address.	📄 Records using “+all”, “?all” or that have a PTR directive are not considered compliant with the Standard. You can test your record at this unaffiliated site: http://www.dnsstuff.com/
Your email operates in a secure environment that does not route through open relays or open proxies	If you are not sure about your security practices, you should check with your email or system administrator.
You participate in Windows Live HotmailJMR feedback loop to reduce complaints. Participation in other available feedback loops is strongly recommended but not required.	📄 If you do not know if you are participating in Microsoft’s MR feedback loop program, you should check with the person responsible for maintaining your mailing list. You can find out how to sign up for feedback loops by visiting: www.returnpath.net/internet-service-provider/feedback
You actively process 550 5.1.1 bounces and remove unknown users from all mailing lists	📄 If you do not know if you are processing bounces, you should check with the person responsible for maintaining your mailing list.

How many messages do you send per month?

You’ll need to know this information before your apply.

Sender Best Practices

The questions below focus primarily on privacy, disclosure and consent. We want to make sure you are following the very best practices when it comes to setting expectations and maintaining the subscriber experience.

Best Practices Standards	Application Tips
Your website provides clear and conspicuous disclosure at the point of collection of email addresses describing the type of email subscribers will receive.	You will also be asked to provide the URLs where a subscriber could sign up and agree to your terms of service. These could include your website, landing pages, registration pages, etc. If you receive subscriber email addresses from third parties, affiliates, or co-registration partners, please also provide the URLs that these parties use to collect subscriber email addresses.
You publish a Privacy Policy which is linked clearly and conspicuously from the front page of the homepage and also from any point of collection.	You will have to provide the URL to your company’s privacy policy on the application and tell us: <ul style="list-style-type: none"> • Whether you share or rent email addresses or personal information. • How subscriber information is being stored, used or shared. • How subscribers can easily opt in/out of your program.
You use only the following forms of consent: Double Opt-In, Opt-In with Verification, OpIn, Pre-selected Option with Verification, Pre-selected Option	You will have to select ALL of the different types of consent you use for your email program. You will choose from the following: Double Opt-In, Opt-In with Verification, Opt-In, Pre-selected Option with Verification, Pre-selected Option or Other. The following forms of consent are not eligible for Return Path Certification: Unselected Opt-Out, dictionary attacks, or harvesting. Additionally, you will have to select ALL of channels you use to collect subscriber consent. You will choose from the following: Online / Electronic, Offline / Written, Verbal, Through Third Parties or Affiliates (list brokers, third party marketing lists, co-reg)
You actively monitor abuse@ and postmaster@ accounts for the FROM and RETURN-PATH domains present in mail headers.	Check with your email or system administrator to find out if this is being monitored.
Your contact information is visible via Whois and is up-to-date.	Note: The use of a Privacy Service to list Whois Records is not allowed.
Every commercial email you send includes a functional, conspicuous and clearly labeled Unsubscribe link and all peer-initiated email includes global Unsubscribe functionality.	You can find out if you comply by looking at your email streams to ensure there is a “one-click” opt-out mechanism clearly labeled and easy to find in each email you send.



If you are a non-profit organization, please have your non-profit tax registration number handy.

Minimum Standards & Requirements

There are seven key standards that senders must meet in order to be admitted to the Return Path Certification program. These same standards must be maintained to remain enrolled in the program.

How to become a Safe sender: Program Standards

The Return Path Certification program's main objective is to identify email senders who follow industry best practices and send relevant, engaging and wanted email to subscribers with whom they have an existing relationship. Only senders with the best email practices will be certified. The program employs many specific standards, metrics and requirements to measure and enforce these practices, though ultimately the decision to certify a sender rests solely with Return Path, and will be guided by the spirit and principals of email certification.

I. Accountability & Measurability

- A. Program Members must ensure that the mail infrastructure used to send email messages is maintained and operated in a responsible manner.
- B. Dedicated IPs Address(es). There must be a dedicated IP address(es) for sending email messages through Return Path Certified. Program Members must be the only entity sending email messages over the IP address(es) for which the Program Member is certified. In addition to a sender's certified IPs, behavior of any third party partners will reflect on your reputation as an email sender, may affect your program status, and may be grounds for termination.
- C. Certified Metrics. Return Path calculates sender reputation metrics which Program Members must meet for all IP address(es) enrolled in the Certified Program. Thresholds for sender reputation metrics are defined in Exhibit A, Quantitative Requirements and include but are not limited to: complaint rates, listings on blacklists, spam trap hits, and unknown user rates. Impact upon our receiving network partners will be taken into account when allowing continued certification, even if complaints are within published limits.
- D. Safe Metrics. Safe IPs must meet published thresholds for the following sender reputation metrics: listings on blacklists, spam trap hits, and unknown user rates.
- E. ISP Targeting. Program Members may not send email to a single receiving source within Return Path's reporting network over an individual IP. It is expected that traffic will be sent to all possible receiving networks. At a minimum, program members must send 30% of their Certified email traffic to each Microsoft/Hotmail and Yahoo!. Occasional and temporary single-receiver mailings will be tolerated under special circumstances, but must be approved in writing by Return Path.
- F. Measurable Volume. Clients must maintain measureable volume on IPs for them to remain whitelisted. In order for us to maintain certification on an IP, at least 100 email messages on any individual source must be seen in our reporting network in a 30 day period, IPs without measurable volume may be suspended after 30 days, and deleted from the program after 90 days.



Do these standards ever change?

Return Path Certification periodically reviews program standards to ensure it remains the highest quality program of its kind and continues to meet the needs of both senders and receivers as email technology evolves. Updates to the program standards may accommodate changes in the email industry, such as to account for the rise of peer-initiated email, or when a new blacklist becomes available. Important industry standards that are adopted by our receiver network may also precipitate an update to the program standards. These updates are rare and senders are always given adequate notice, so there are no surprises.

G. List Maintenance. Email address list maintenance systems must be employed to reliably receive and process delivery errors, bounce messages, and other replies from receiving networks. Permanent delivery errors from email messages sent over IP address(es) enrolled in Return Path Certification must be processed by removing the undeliverable email address from all future mailing.

H. rDNS. The IP address(es) enrolled in Return Path Certified and Return Path Safe must have fully qualified Reverse DNS entries. The rDNS policy requirement means a sending IP address

must have a valid pointer (PTR) record in the Domain Name System (DNS) which resolves to a valid hostname. That hostname must then have an address (A) record in DNS which includes the sending IP address.

I. Single Domain Name Servers. Return Path looks for a typical distribution of servers to domains. Domains should not be hosted on single-domain name servers. For example, the following is not in keeping with RP Certification services standards of transparency.

domain1.com – ns. domain1.com
 domain2.com – ns. domain2.com
 domain3.com – ns. domain3.com

J. Hostnames should clearly identify the sending entity, by variations appended to a limited number of domains, and related to the sending entity. For example, the following is not an acceptable deployment:

mx.senderhost1.com
 mx.senderhost2.com

Whereas the following is an appropriate deployment, using sub-domains:

mx1.senderhost.com
 mx2.senderhost.com

K. The HELO server name must match the rDNS of the sending IP address, and must be presented in the form of a domain name, not an IP address. HELOs must remain consistent for the duration of given campaign, and should remain the same for subsequent campaigns.

L. Netblocks. IP Groups should contain no more than three discrete netblocks. Requests for exceptions to this standard must be submitted in writing to Return Path accompanied by a comprehensive rationale and description of the use of all IPs, both existing and proposed.

M. RFC Compliance. Program Members must be compliant with Request for Comment (“RFC”) Numbers 5321 and 5322, which describe how email messages must be formatted in order to be processed properly by receiving networks. Forward to a friend email messages must be compliant with RFC 2822 “sender: header” specifications.

N. Physical Address. Program Members must include their valid physical mailing address within all Commercial or Promotional Messages.

Racing Post says...

“Since joining the Return Path Certification program, we have seen a dramatic increase in both deliverability and response. At Hotmail, we achieved a 276% increase in open rates and doubled our click through rates. As an added benefit, our unsubscribes and complaint rates significantly decreased which means we have more engaged readers. Now, we consistently reach our customer and prospect inboxes and realize an increased ROI for each campaign. Return Path’s Certification program is well worth it.”

- Lucy Watson, Marketing Manager at Racing Post

II. Transparency and Authentication

- A. Program Members must ensure that email messages are truthful and accurately identify the source of the message.
- B. SPF. A Sender ID compliant SPF record must be published for all domains from which email messages are sent
- C. DKIM. DomainKeys Identified Mail (DKIM) authentication will be required effective March 1, 2011 for all email messages sent over certified IPs.
- D. Message Headers. email message headers must not be falsified, obscured, deceptive, or misleading in any way. This includes, but is not limited to, the Return-Path header, the From: header, and the friendly part of the From: header.
- E. Content. The subject line and body content of email messages must not be falsified, obscured, deceptive or misleading in any way.
- F. All IP blocks greater than 8 IP addresses must be SWIPed in keeping with RFC 1491 to indicate ownership by the Program Member.

III. Security

- A. Program Members must ensure that adequate, industry standard policies and procedures are in place to secure and protect Recipients' email addresses and Related Personal Information held in databases or on electronic systems.
- B. Adequate, industry standard efforts must be made to prevent open proxies, open relays and computer viruses, worms, spyware, adware, trojans, recursive DNS or any other item deemed malware in the Program Member's mail infrastructure.
- C. When undertaking address book uploads, the only acceptable method is with Application Processing Interfaces API). Several receiving sites provide this facility, including:

AOL = <http://dev.aol.com/openauth>

Google = <http://code.google.com/apis/accounts/AuthForWebApps.html>

Yahoo = <http://developer.yahoo.com/auth/>

Windows Live Contacts = <http://dev.live.com/contactscontrol/default.aspx>

IV. Privacy Policy

- A. Program Members must ensure that all privacy policies referenced at applicable point of collection websites accurately and completely reflect the actual practices of the Program Member.
- B. The practices reflected in a privacy policy must be equally reflected in the Disclosure statements made at the point of collection.
- C. Must be clearly, conspicuously and directly referenced at all points of collection.
- D. The privacy policy must include clear and unambiguous instructions on how to unsubscribe from future email messages.
- E. The privacy policy must include a mailing address, and email address, and telephone number.

A Leading Health Services Provider says...

"Since working with Return Path we've been able to improve our reputation and consequently our overall deliverability, but we were still having trouble at Hotmail/MSN – a key domain for us. The benefits of being part of the Certification program immediately provided us with 100% deliverability to Hotmail/ MSN and that deliverability rate has remained consistent since our acceptance."

-Manager, Consumer Marketing, Product and Channel

V. Disclosure and Consent

A. Disclosure

- i. Program Members must ensure that clear and conspicuous disclosure is made at the point of collection of Recipient email address and Related Personal Information. A link to a privacy policy is insufficient.
- ii. Program Members must clearly disclose the nature of Commercial or Promotional email messages to be sent.
- iii. Program Members must clearly disclose their practice of sharing or renting of the Recipient's email address and/or Related Personal Information at the point of collection. Program Members must clearly disclose actions that will result in additional Commercial or Promotional email messages from Affiliates and/or Third Parties.

B. Consent

- i. Program Members must ensure that consent with appropriate disclosure or a prior business relationship exists prior to sending Commercial or Promotional email messages. Acceptable forms of consent include:
 - a. Double Opt-In: (sometimes referred to as 'Confirmed Opt-In'): The Recipient affirmatively requests to add his/her email address to a mailing list. The Recipient receives a confirmation email and the Recipient confirms his/her request by replying or visiting a provided URL.
 - b. Opt-In with Verification: The Recipient affirmatively requests to add his/her email address to a mailing list. The Recipient receives a verification email notifying him/her of the subscription and providing clear unsubscribe instructions.
 - c. Opt-In: The Recipient affirmatively requests to add his/her email address to a mailing list.
 - d. Pre-Selected Opt-In with Verification: The recipient consents to have his/her email address added to a mailing list by leaving a clear and conspicuous pre-selected option intact. The recipient receives a verification email notifying him/her of the subscription and providing clear unsubscribe instructions. Commercial or promotional email messages sent under this form of consent must include clear and conspicuous identification that the message is an advertisement or solicitation.
 - e. Pre-Selected Opt-In: The recipient consents to have his/her email address added to a mailing list by leaving a clear and conspicuous pre-selected option intact. Commercial or promotional email messages sent under this form of consent must include clear and conspicuous identification that the message is an advertisement or solicitation. However, this practice is not permitted for co-registration.
- ii. Prior Business Relationship. A prior business relationship exists where (1) the Recipient has purchased a product or service from the Email Address List Owner within the past 18 months, (2) the Recipient consensually provided his/her email address and (3) the Recipient has not unsubscribed or opted out from Commercial or Promotional email messages, or otherwise terminated the relationship. An Affiliate or Third Party may not rely on a prior business relationship for sending Commercial or Promotional email messages.
- iii. Co-Registration. The following requirements must be met to be considered a co-registration:
 - a. The Program Member that acquires the email addresses was explicitly, clearly, and conspicuously named at the point of email address collection;
 - b. Each act of consent (e.g., a check box) resulted in the addition of an email address to only one list; 3. Proof of consent, including the date, time, originating IP address, and location (e.g., a URL) where the address collection occurred can be produced by the Program Member upon request.
 - c. Pre-Selected Opt-In is not permitted as an acceptable form of consent for Co-registration sign-ups.
 - d. Obtaining and distributing of any email addresses collected on the certifiable sender's website must also meet these requirements.

- iv. Exceptions to Consent Requirement for Peer-Initiated Communication - Commercial or Promotional email messages.
 - a. A Program Member may send one Peer-Initiated Commercial or Promotional email message to an individual whose email address has been referred to it by a Recipient without that individual's consent. The mere referral of an individual's email address is not consent by that individual to receive Commercial or Promotional Emails from the Program Member. Headers of these email messages must clearly and accurately reflect the Program Member.
 - b. Program Members that send Peer-Initiated Commercial or Promotional email messages must employ one of the methods for obtaining consent provided in section v. b, in order to obtain an individual's consent for Commercial or Promotional email messages other than the Peer-Initiated Commercial or Promotional email message.
 - c. An individual's failure to respond to a Peer-Initiated Commercial or Promotional Email Message may not be construed as that individual's consent to receive email messages from a Program Member. If the individual does not respond, the Program Member may send one follow-up email message soliciting that individual's consent for Commercial or Promotional email messages from the Program Member. If the individual does not respond to the follow-up email message, the Program Member may not send any additional Email messages to him or her.
 - d. A Program Member is free to send as many peer-initiated commercial and promotional messages as the individual peer wants to initiate, unless and until the recipient opts out.
- v. Prohibited Consent Practices:
 - a. A Program Member may not send email messages to email addresses that have been obtained by harvesting, dictionary-style attacks or through any means which do not meet one of the above acceptable forms of consent.
 - b. List rental, purchase or email append are not acceptable forms of consent.
 - c. A Program Member is free to send as many peer-initiated commercial and promotional messages as the individual peer wants to initiate, unless and until the recipient opts out.

VI. Unsubscribe

- A. Program Members must ensure that the Recipient's requests to discontinue receipt of Commercial or Promotional email messages, or Peer-Initiated Email messages, are honored.
- B. Every Commercial or Promotional email message, and every Peer-Initiated email message, sent under these Program Requirements must include an Unsubscribe option. Removal instructions must be clear, conspicuous and easily understood. This should be as close to a 'one-click' process (such as selecting a URL) as possible.
- C. All unsubscribe mechanisms must adhere to the following:
 - i. Easy to Use: Unsubscribe mechanisms may include a reply to the Commercial or Promotional email message sent to the Recipient or an online process described in that Commercial or Promotional email message with a URL. The Unsubscribe process must not require a Recipient to provide any information other than the Recipient's email address
 - ii. Timely: A Recipient's request to unsubscribe must be processed, and the request must become effective within 10 days from receipt.
 - iii. Persistent: Unsubscribe mechanisms must be functional for at least 60 days following the sending of the Commercial or Promotional email message.
 - iv. Indefinite: A Recipient's request to unsubscribe is valid and must be honored indefinitely, or until the Recipient provides his or her new consent, as defined in these Program Requirements, to receive Commercial or Promotional email messages.

- v. Absolute: Once a Recipient has unsubscribed, Commercial or Promotional email messages may not be sent and the Recipient's email address or related personal information may not be sold, leased, or otherwise shared with Third Parties.
- vi. Flexible: If a Recipient contacts the Sender with an 'Out of Band Request' for an unsubscribe, for example, via postal mail, email to another account at the Sender (e.g., abuse@sender.domain or postmaster@sender.domain), or through a telephone call, those unsubscribe requests should be acted on in a timely manner.
- vii. All emails must be CAN-SPAM compliant. All such emails from which a subscriber should have the ability to unsubscribe, as specified under CAN-SPAM must also include the List Unsubscribe header as specified under RFC 2368.

VII. Message Content

- A. Email messages containing solely 3rd party marketing are not eligible for Certified status. These messages are eligible for Safe status, and must be clearly and conspicuously branded as being from the Program Member.
- B. 1st party email messages that contain 3rd party content (ad-sponsored) are eligible for Certified, but must meet the following requirements :
 - i. All email messages must be clearly and conspicuously branded as coming from the named (Certified) sender.
 - ii. The 'from' address and 'friendly from' must be identified as the named (Certified) sender.
 - iii. The subject line must reference the 1st party content included in the message.
 - iv. 1st party content must be both original and predominant in proportion to the advertisements.
- C. Senders who send both 1st and 3rd party content are eligible for Certified status for their 1st party IPs, and eligible for Safe status for their 3rd party IPs.
- D. Senders of 1st Party content are eligible for both Certified and Safe status.

VIII. Responsiveness

- A. Program Members must ensure that all parties involved in the sending of email messages cooperate with program administrators to resolve any issues regarding Program Requirements by responding in 3 days of notice, and by taking corrective action within 10 days of notice.
- B. Program Members must create and maintain the standard role email accounts abuse@sender.tld and postmaster@sender.tld for all domains that appear in message headers in order to facilitate handling complaints and other issues. It is strongly recommended that standard role email accounts also be supported for Sender controlled domains appearing in the message body.
- C. Program Members must maintain accurate contact information in the whois database and no privacy protection services may be used for all Sender controlled domains that appear in message headers and body text, are used for user sign-up, preference and unsubscribe sites.
- D. Sender agrees to maintain current and correct contact information with Return Path.



How do you know so much about my email?

Return Path has developed the industry's largest collaborative email reputation data network. Participating ISPs and filtering companies contribute data about your email into our data network. This data comes from entities such as Microsoft, Yahoo!, Lashback, as well as additional anonymous sources that Return Path is obligated to keep confidential. Other data is obtained from public sources such as blacklists.

How to become a Certified sender:

Senders with superior sending reputations may be upgraded to the Certified level. To become (and remain) a Certified sender, you must meet superior performance and reputation standards in addition to the minimum standards listed above. Performance is based on a key set of metrics that have set thresholds for compliance. As a member of the Certification program, you will have access to reports that warn you when your IP addresses are nearing the allowable thresholds so you can proactively make adjustments to your program and avoid interruption to your service.

Certified Level Standards

Metric	Performance Calculation	Rates / Thresholds					
Windows Live Sender Reputation Data	IP addresses are evaluated and enforced when at least 6 total votes are present. Group enforcement applies only to active IP addresses with at least 30 total votes present. Group enforcement will only apply to IP address with at least 1 SRD Junk Vote.	SRD Volume	SRD Volume	SRD Volume	SRD Volume	SRD Volume	
		6 to 9 50%	10 to 19 45%	20 to 39 40%	40 to 99 35%	99+ 30%	
Hotmail Complaint Rate	Receiver Complaint Rates are determined by dividing the number of complaints generated by the volume of mail accepted for delivery. Each receiver provides actual accepted volume and actual complaint volume.	Volume Sent: to 2 million 2.9%	Volume Sent: 2 million to 10 million 1.8%	Volume Sent: 10 million to 85 million 0.8%	Volume Sent: 85 million plus 0.4%		
Yahoo! Complaint Rate		Volume Sent: to 5 million 2.0%	Volume Sent: 5 million to 20 million 1.5%	Volume Sent: 20 million to 100 million 1.0%	Volume Sent: 100 million plus 0.8%		
Comcast Complaint Rate		Volume Sent: to 92,000 1.1%	Volume Sent: 5 million to 20 million 0.6%	Volume Sent: 20 Million plus 0.2%			
Source B Complaint Rate		Volume Sent: to 92,000 1.1%	Volume Sent: over 92,000 0.35%				

Unknown User Rate	An 'unknown user' or 'no such user' or 'invalid address' is a 550 5.1.1 error message that will appear in your bounce logs. The Unknown User rate is calculated by dividing the number of these transactions as reported by Source B by the actual volume of mail attempted for delivery at Source B.	10%
Spam Traps	Spam trap hits are reported on an absolute volume basis.	1 Critical trap hit 5 Significant trap hits
Blacklists	A listing is defined as a unique occurrence on a top tier DNSBL blacklist. Senders listed multiple times on the same blacklist will be assessed based on number of occurrences.	1 Critical listing 2 Significant listings

*All metrics are averaged and totaled (as applicable) based on data collected over the previous 30 day period. This accounts for daily variation in the data while capturing recent trends.



More About Complaint Rates

Complaint rate thresholds are designated by your monthly email volume. Rates vary by receiver and are based on a statistical analysis that accounts for, among other things, how a receiver solicits complaints.

Your allowable complaint rate is based on the number of messages you attempt to send to either Hotmail, Yahoo! Comcast or Source B. The more mail you attempt the send, the lower your allowable complaint rate. Your attempted mail volume includes all mail that you send to the receiver for processing and does not take into consideration bounces and other such reasons that mail is rejected.

Higher-volume senders have lower allowable complaint rates because they have the potential to cause greater damage to receivers even if it's just a small increase. Therefore, higher volume senders must behave more responsibly to minimize both absolute and relative complaints. This is not to say that low volume senders are off the hook. Their complaints just have different effects on receiver systems. Complaints rates are still enforced no matter how much mail you send. Each metric and client is reviewed on a case-by-case basis and we will make exceptions where warranted and applicable.

Best Practice Guide: Improve Your Chances for Success

Our goal is help create world class senders. In this section we've outlined the best practices that 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 un-subscribe functionality is compliant. These elements are the core components of 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 SpamNet) or a complaint-driven blacklist like SpamCop.
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



Check Your Sender Score.

When was the last time you checked your Sender Score?

Check it daily at www.senderscore.org or in Reputation Monitor if you are already a Return Path client. Like a credit score, your Sender Score is an indication of the trustworthiness of your mail streams.

The higher your score, the better your deliverability should be. And while a Sender Score can't guarantee you premium placement in the inbox, it's a great indicator of a potential problem.

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.)



Premium Benefits

A premium benefit of being a Certified sender is that email sent over certified IP addresses to Hotmail will have a trusted unsubscribe link when you use a list-unsubscribe header.

You can find more information about implementing the list-unsubscribe header at: www.list-unsubscribe.com.



Visibility Into Your Email Deliverability

Return Path provides deliverability monitoring tools that will provide visibility into your email deliverability. With our comprehensive tools, you can find out exactly which campaigns or customer segments are generating the most complaints and take action.

We can also help you sign up for all of the feedback loops. And if you need more consultative service, we can provide a strategic recommendation and an action plan to reduce your complaint rates for the long haul.

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:

- **SpamCop 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.



Clear Visibility Into User Rates

Return Path's deliverability monitoring tools can provide clear visibility into your unknown user rates. Analysis of Return Path senders indicates that mailers with strong data hygiene practices can attain unknown user rates of less than 2% on a consistent basis

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.

APPENDIX

Definitions

550 5.1.1 entry: An 'unknown user' or 'no such user' or 'invalid address' is usually a '550 5.1.1' error message that will appear in your smtp logs however, not all ISPs use the '5.1.1' extended reply code, and not all '550' replies refer to unknown users. It is often necessary to review the text accompanying that SMTP reply to be certain of its meaning.

Affiliate: The term "affiliate" means an entity that is not connected to the participating sender by a common marketing brand, but is related to the participating sender by corporate or organizational structure.

Commercial or Promotional Email Message: The term "commercial or promotional email message" means any electronic email message that is business-related or an endorsement and is sent by the participating sender or on behalf of the participating sender other than: a transactional or relationship email message, or a personal correspondence email message. Examples of commercial or promotional email messages include, but are not limited to marketing messages, promotional messages, fundraising messages, newsletters, and surveys.

Co-Registration: Co-registration is the practice of mailing to email addresses that are collected from a checkbox specifically naming your company on a website you don't own or operate rather than a direct signup.

Email Address List Owner: The term "email address list owner" means a company, company division, subsidiary, co-branding partner, or organization that is connected together by a common marketing brand and owns the list of email addresses that is being used under these program standards.

Email Append: Email appending is the process of merging a database of information on individuals containing information other than the individuals' email addresses, with a service provider's database of email addresses in an attempt to match the email addresses with the information in the initial database.

Email Message: The term "email message" means any email that is sent by the participating sender or on behalf of the participating sender.

First Party Content: First Party content email messages promote the sender's own products or services, or provide a service within the email message, such as transactional notices or email newsletters.

HELO: HELO is the SMTP command greeting that is initiated to the receiving MTA and contains its FQDN.

Internet Message Format: The Internet Message Format (IMF) is a syntax for text messages that are sent between computer users, within the framework of email messages.

Internet Protocol (IP) address: IP address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Each computer that sends out email has an IP address.

List Rental: The term "List Rental" refers to the practice of mailing to email addresses that are rented and/or purchased via a third party list broker.

Netblocks: A Netblock is a range of consecutive IP addresses.

Network Working Group RFC2821: RFC 2821 is a document specifying the original Simple Mail Transfer Protocol (SMTP) for email messaging.

Participating Sender: The term "participating sender" means a company, company division, subsidiary, or organization that signs the Return Path Certification license agreement. In instances where the participating sender did not collect the email addresses directly, but rather is acting as an agent for the email address list owner, the participating sender must ensure that the program requirements are satisfied by the email address list owner.

Peer-Initiated Commercial or Promotional Email Message: The term “peer-initiated commercial or promotional email message” means a commercial or promotional email message that is sent by the participating sender, or on behalf of the participating sender, to an email address provided by a recipient who has requested that the participating sender contact an individual other than the recipient for the purpose of informing that individual about the participating sender’s product(s) or service(s).

Point of Collection: A Point of Collection (POC) is the place on a website where email addresses are collected and subsequently mailed to.

rDNS: Reverse DNS (RDNS) translates the sending server IP address into its hostname (host.example.com) by searching domain name service tables. RDNS is important because many email servers are configured to reject messages from senders with no RDNS. Specifically, AOL will reject any incoming mail with no valid RDNS.

Recipient(s): The term “recipient” means the individual who receives an email message covered by these program requirements.

Related Personal Information: The term “related personal information” means other personal information provided by the recipient at the time of email address collection.

Sender ID: Sender ID is an email authentication system from Microsoft that’s based on Sender Policy Framework (SPF) records in the DNS system. To validate a Sender ID the first thing that happens is the Purported Responsible Address (PRA) domain is determined. In most cases the PRA will be the “From:” address so the “From:” domain is what’s typically determined as the PRA domain and used to validate the sender. The next step is to validate whether or not the sending IP is authorized to send mail from this domain. It does this by looking in the DNS for an spfv2 record for the domain and verifying the IP is listed (results provided above). If no spfv2 record is present, Sender ID will look to the spfv1 record and look up the domain to verify the IP is authorized.

Most ISPs checking Sender ID will fall back to the SPF record and if it passes then you’re okay. Sender ID will mostly affect your ability to get mail delivered at MSN and Hotmail. There are publically available DNS testing resources, including: <http://www.dnsstuff.com/>. If you’re failing the Sender ID test, refer to Microsoft’s Sender ID Resources page which will walk you through setting one up.

Spam Traps: Spam traps are email addresses that are set up specifically to catch mailers who are harvesting addresses or using directory attacks to send unsolicited email.

SPF (Sender Policy Framework): is an email authentication system that verifies that the message came from an authorized mail server. If so, it verifies if the sending IP address is allowed to send mail for the sending domain. The SPF check is performed on the “Return-Path:” domain not the “From:” domain. Most major ISPs check for SPF records and will usually place your email in their junk folder (or equivalent) without one.

There are publically available DNS testing resources, including: <http://www.dnsstuff.com/>. If your SPF record is failing, or you don’t have an SPF record, there’s a great set up wizard that will walk you through setting one up. <http://old.openspf.org/wizard.html> Once your record is ready to be published, you publish as a record of type TXT in your domain’s public DNS. If you don’t know how, you will need to contact your DNS provider. In most cases, this will be the system administrator in your IT department.

Simple Mail Transfer Protocol (SMTP): is an Internet standard for email transmission across Internet Protocol (IP) networks. SMTP was first defined in RFC 821 (STD 10), and last updated by RFC 5321 (2008) which describes extended SMTP (ESMTP), the protocol in widespread use today.

SWIP: SWIP is the process that Internet Service Providers (ISPs) use to submit customer IP space reassignment information to WHOIS. The purpose of SWIP is to ensure effective, efficient maintenance of records on IP address space.

Third Party: Third Party content email messages promote the products or services of another company.

tld: Top level domain.

Transactional or Relationship Email Message: The term “transactional or relationship email message” means any electronic mail message sent by the participating sender or on behalf of the participating sender the primary purpose of which is:

1. to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the participating sender;
2. to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;
3. to provide any of the following regarding a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the participating sender:
 4. notification concerning a change in the terms;
 5. notification of a change in the recipient’s standing or status; or
 6. at regular periodic intervals, account balance information or other type of account statement.
7. to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or
8. to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

Windows Live Hotmail JMR: This is Microsoft Hotmail’s Feedback Loop program. The Junk E-Mail Reporting program (JMR) is a Microsoft program intended to help large senders remove unwanted recipients from their e-mail lists. The goal of this program is to clean-up distribution lists so that users receive wanted e-mail and senders aren’t negatively affected by complaints. Senders that sign up for this program will receive any e-mail that is reported as junk e-mail. If you are not sure if your company is signed up to receive feedback from Microsoft, check with the person responsible for maintaining your mailing list.