

## Minimum Level 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 found above in the Certified Level Standards 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 measurable volume on IPs for them to remain white listed. 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.
- 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.

## 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 is required 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.

#### 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. Any form of email prospecting, i.e., where there is no consent or existing business relationship between the sender and the recipient, such as opt-out, is not permitted.

## 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.
  - viii. In the case of Peer-Initiated Communications, the unsubscribe must allow Recipients to unsubscribe from all future email messages from the Program Member, whether Peer-Initiated or not.

## 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.

## Certified Level Standards

Values in the chart below are the maximum thresholds for membership in good standing. Any data metric in excess of these thresholds will be considered out of compliance with Certified level standards.

<b>Windows Live Sender Reputation Data</b> (30 day average)	Both group and individual IP addresses are evaluated for compliance with the standard. Groups and IP addresses are considered to be compliant with this standard if the percent voted spam is less than 50%.			
<b>Microsoft - Hotmail: Complaint Rate</b> (30 day average)	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%
<b>Yahoo!: Complaint Rate</b> (30 day average)	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%
<b>Comcast: Complaint Rate</b> (30 day average)	Volume sent: to 5 million 1.1%	Volume sent: 5 million to 20 million 0.6%	Volume sent: 20 million plus 0.2%	
<b>Source B: Complaint Rate</b> (30 day average)	Volume sent: to 92,000 1.1%	Volume sent: over 92,000 0.35%		
<b>Unknown User Rate</b> (30 day average)	10%			
<b>Spam Traps</b> (30 day cumulative)	1 Critical trap hit 5 Significant trap hits			
<b>Blacklists:</b> (Current listing)	1 Critical listing 2 Significant listings			

## Definitions

**Affiliate:** The term “Affiliate” means an entity that is not connected to the Program Member by a common marketing brand, but is related to the Program Member 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 Program Member or on behalf of the Program Member. It could include but is 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 Program Member or on behalf of the Program Member.

**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.

**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.

**Peer-Initiated Commercial or Promotional Email Message:** Peer-initiated communications are emails sent from one user to another. Social networks facilitate peer-to-peer communication in the form of friend requests and notifications.

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

**Program Member:** The term “Program Member” means a company, company division, subsidiary, or organization which contracts with Return Path. In instances where the Program Member did not collect the email addresses directly, but rather is acting as an agent for the Email Address List Owner, the Program Member must ensure that the Program Requirements are satisfied by the Email Address List Owner.

**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.

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

**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:** The term “Third Party” means a commercial entity that is unrelated by corporate structure to a Program Member and that is not acting as the Program Member’s agent.

**Third Party Content:** 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 Program Member or on behalf of the Program Member the primary purpose of which is:

- i. to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the Program Member;
- ii. 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;
- iii. 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 Program Member:
  - a. notification concerning a change in the terms;
  - b. notification of a change in the recipient’s standing or status; or
  - c. at regular periodic intervals, account balance information or other type of account statement.
- iv. to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or
- v. 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.