Certification

Standards and Requirements

December 2017

Return Path, Inc.

Table of Contents

Introduction

What are the standards and requirements for becoming and staying Certified?

Return Path Certified senders follow industry best practices and send relevant email to subscribers who want it. They are the best-of-the-best mailers who agree to maintain the high standards required of them.

This document lists all standards required for compliance. Failure to live up to these standards may cause suspension from the whitelist, or removal from the program. Please note that Certification program members must make sure anyone involved in the sending of email messages cooperate with Return Path Certification staff to resolve any issues about program requirements by responding in 3 days of notice, and by taking corrective action within 15 days of notice. Though 15 days is the cure period for taking corrective action, please note that Return Path reserves the right to suspend customers immediately for violation of the Program Standards.

Why do we hold senders to these standards and requirements?

Each of these requirements represents one of six underlying sending behaviors. These requirements make sure that you, as a Certified sender:

- Remain **measurable**: or allow us to accurately measure your reputation and performance by sending consistent, measurable volume and *only* sending mail you own.
- Be **transparent and accountable**: or be who you say you are, do what you say you're going to do, and stand behind the mail you send by remaining easily reachable.
- Have **clear disclosure**: or give your subscribers a clear appreciation and understanding of how you will use their email addresses or personal information.
- Use **good consent** practices: or mail to subscribers who want your mail — and let people out if they don't want your mail anymore.
- Keep up with **security** measures: or take adequate, industry-standard steps to keep your database and systems secure, so you can protect your infrastructure and your subscribers.
- Meet **performance** requirements: or remain within Certification compliance metrics by following industry best practices for complaints, unknown users, spam traps, and blacklists.

If you do not consistently display these sending behaviors, mailbox providers may think you're a spammer. Also, your Certified program status may be up for review.

Measurability

Allow us to accurately measure your reputation and performance by sending consistent, measureable volume and only sending mail you own.

Dedicated IP Address

What is a dedicated IP address?

Dedicated IPs are those used by a single sender or company. Shared IPs are dynamic and can be used by thousands of senders.

Why am I required to send from a dedicated IP address?*

Mailbox providers base sending reputation off IP traffic. You can only control your reputation and status in the Certification program by sending from dedicated IPs. If you do not, the metrics Certification monitors will not be accurate. So, you can't share traffic on Certified IP addresses — even with organizations you have a relationship with.

* For senders using shared IPs, domains can be accepted into the Certification program if they are are authenticated with DomainKeys Identified Mail (DKIM). See the Addendum at the end of the document for all of the details of the Domain Certification program.

Measurable and Consistent Volume

What is measurable volume?

In our program, measurable volume means 200 email messages (100 to Yahoo! and 100 to Microsoft) sent in a 30-day period from each Certified IP.

Also, the number of IPs senders own — and have Certified — should be relative to the volume they send.

What is consistent volume?

In our program, consistent volume means IPs have been used consistently for at least 60 days.

Why do I need to maintain measurable and consistent volume for each Certified IP?

We can only effectively monitor IPs sending measurable volume. Also, IPs with zero sending volume present security issues.

IPs without measurable volume will be suspended after 30 days and removed from the program after 60 days.

Mailing to a Single Mailbox Provider

Why can't I mail to only one mailbox provider from one Certified IP?

Certified senders cannot segment traffic by mailbox provider from one Certified IP. Because this behavior is often used by senders to avoid or obscure reputation data or program measurements, it is only allowed in special circumstances, and only if approved in writing.

Senders who use these tactics, or similar ones, may have their IP address suspended or their account removed from the program.

Sending Third-Party Mail

What is third-party mail?

Third-party mail is email that refers to another company's domains or content.

Companies typically send this type of email because they have a business relationship with another company, or because they are an ESP or agency that sends email on behalf of clients.

Why can't I send third-party mail?

Sending mail for third parties introduces potential issues with security, list hygiene, disclosure, consent, and more.

Third-party messages sent by the client's domains can confuse recipients so they may mark the email as spam — and negatively affect performance metrics.

Also, third parties are not covered under your contract.

We certify one entity (the parent company that owns the mailing program) per application.

Because these third parties have not applied to and been accepted into Certification, they cannot benefit from the service.

Are there any exceptions to the third-party sending rule?

Under some circumstances, Certified senders may include third-party content only if the email's subject line, Friendly From, and Mail From domains name you, the Certified sender — and if your content is more prevalent than theirs.

Example of an acceptable email including third-party content

Certifiable Business Models

What is a Certifiable business model?

Certified senders must be a part of a company that has a Certifiable business model. This includes businesses that do not send third-party content or act on behalf of clients.

What is an Uncertifiable business model?

Uncertifiable business models include companies sending:

- Mail on behalf of clients (such as ESPs, hosting companies, or agencies)
- Corporate mail
- Mail from a shared IP
- Third-party content

Why are those business models Uncertifiable?

We cannot certify ESPs, hosting companies, or agencies because they send third-party mail. Certified senders need to own their own email program and have the ability to make changes to it. Also, Certified senders are audited and accepted on a per-company basis.

We cannot certify corporate mail because it allows for too many potential points of entrance and, therefore, opens risks for security, consent, and measurability.

For why sending third-party content and using shared IPs is not allowed, see the Sending Third-Party Mail and Dedicated IP Address sections.

Are there any exceptions to the Certifiable business model rule?

Certified senders can have clients with accounts, such as a social media entity that sends peer-to-peer messaging.

Legally Registered, Established Businesses

What is a legally registered, established business?

Legally registered, established businesses are sound, secure companies. Certified sender mailing programs must belong to this type of business.

To prove this, Certified sender businesses must:

- Be legally registered
- Have a physical address
- Have been operational for a minimum of one year
- Be verifiable by a third-party source such as [yourstate].gov or WhoIS.com

Also, Certified business entities (brand parent companies) must also be legally registered and have been operational for a minimum of six months.

Why do I need to have a legally registered, established business?

Businesses, brands, and mailing programs inevitably experience many changes in their first few months.

So that Certification analysts can reliably vet a sender's application, their business, brand, and mailing program needs to be legally registered and established for the minimum amounts of time as previously stated.

What if my business or email program experiences a significant change?

If your business goes through a significant change (such as an acquisition) or if you begin sending new or different categories of mail from Certified IPs, you must notify Return Path in advance.

To do so, email certification@returnpath.com.

Transparency and Accountability

Be who you say you are, do what you say you're going to do, and stand behind the mail you send by remaining easily reachable.

Truthful, Accurate Representation

Why do I need to represent myself truthfully and accurately?

We, along with our data partners, expect that Certified senders will be easily reachable and proudly stand behind mail sent. If your email content — including subject lines, headers, and contact information — is hidden, misleading, or deceptive, you may appear as if you are avoiding accountability or ownership.

Also, providing clear and accurate subject lines, headers, and contact information will:

- Help keep your complaint rate down because subscribers know who is sending them mail
- Boost subscriber trust because they can easily reach you with questions, if needed

How do I truthfully and accurately represent myself as a mailer?

To truthfully and accurately represent yourself as a mailer:

- Include a valid physical mailing address within all commercial or promotional messages (required by CAN-SPAM)
- Make sure subject lines tell users what's actually in the email
- Identify yourself or your business in the Return-Path, From, and Friendly-From header domains
- Make sure all content, including links and logos, represent your business
- Have an up-to-date, accurate privacy policy that complies with all laws
- Have an up-to-date, accurate WhoIS record

Privacy Policy

What is a privacy policy?

A privacy policy gives users information about your company's email program, including what you do with their email addresses.

Here is an example of a good privacy policy.

Why do I need a privacy policy?

By telling users what you will do with their emails through a privacy policy that's easy to access and understand, you can build trust with them and improve their customer experience. Plus, you will also remain compliant with email laws such as CAN-SPAM.

What requirements do I need to know for creating or updating my privacy policy?

The Certification program, along with laws regulating commercial email, require that your privacy policy:

- Provides a link with clear unsubscribe instructions for your mail and any of your sending partners' mail (CAN-SPAM)
- Includes a postal address for your company and any partner companies (CAN-SPAM)
- Is linked from all points of collection, including the front page of your website (CalOPPA)
- Tells users what information is gathered and how it might be shared (CalOPPA)

WhoIS Record

What is a WhoIS record?

An internet directory service, WhoIS contains information about a domain name or IP address, such as addresses, phone numbers, and more.

Senders need to have WhoIS records that are set up correctly, have accurate contact information, and do not hide domains behind privacy services.

Example WhoIS records

Here is an example of a complete WhoIS

```
Domain Name: RETURNPATH.COM
Registrar URL: http://www.godaddy.com
Updated Date: 2013-03-04 11:34:11
Creation Date: 1999-02-16 00:00:00
Registrar Expiration Date: 2014-05-01 06:59:59
Registrar: GoDaddy.com, LLC
Registrant Name: Domain Owner
Registrant Organization: Return Path, Inc.
Registrant Street: 304 Park Ave South
Registrant Street: 7th Floor
Registrant City: New York
Registrant State/Province: New York
Registrant Postal Code: 10010
Registrant Country: United States
Admin Name: Domain Owner
Admin Organization: Return Path, Inc.
Admin Street: 304 Park Ave South
Admin Street: 7th Floor
Admin City: New York
Admin State/Province: New York
Admin Postal Code: 10010
Admin Country: United States
Admin Phone: +1.2129055500
Admin Fax: +1.2129055501
Admin Email: domain.owner@returnpath.net
Tech Name: Domain Owner
Tech Organization: Return Path, Inc.
Tech Street: 304 Park Ave South
Tech Street: 7th Floor
Tech City: New York
Tech State/Province: New York
Tech Postal Code: 10010
Tech Country: United States
Tech Phone: +1.2129055500
Tech Fax: +1.2129055501
Tech Email: domain.owner@returnpath.net
```

Here is an example of an incomplete WhoIS

```
Domain Name: USERSUPPORTTEAM.COM
Registrar: MONIKER

Registrant [3836641]:
Moniker Privacy Services USERSUPPORTTEAM.COM@monikerprivacy.net
Moniker Privacy Services
1800 SW 1st Avenue
Suite 440
Portland
OR
97201
US

Administrative Contact [3836641]:
Moniker Privacy Services USERSUPPORTTEAM.COM@monikerprivacy.net
Moniker Privacy Services
1800 SW 1st Avenue
Suite 440
Portland
OR
97201
US
Phone: +1.5032070147
Fax: +1.9545859186

Billing Contact [3836641]:
Moniker Privacy Services USERSUPPORTTEAM.COM@monikerprivacy.net
Moniker Privacy Services
1800 SW 1st Avenue
Suite 440
Portland
OR
97201
US
Phone: +1.5032070147
```

Why do I need a complete WhoIS record?

Certified senders should be easily reachable and proudly stand behind their mail. If your contact information is missing, obscured, or privatized, it can seem that you are dodging responsibility for your mailing program.

What are requirements for my WhoIS record?

Certified senders are required to have a WhoIS record that:

- Is up-to-date
- Has correct information for all domains (associated with Certified IPs) that appear in header or body text

- Has correct information for all domains (associated with Certified IPs) used for subscriber sign-up, preference, and unsubscribe sites
- Contains your legal name
- Lists at least one method of contact
- Contains a mailing address that is not a PO box
- Does not contain a domain by proxy
- Does not list a privacy service

Legal Compliance

What is CAN-SPAM?

CAN-SPAM stands for Controlling the Assault of Non-Solicited Pornography and Marketing Act. It sets laws for commercial email, which it defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." The act established the first national standards for sending commercial email; the Federal Trade Commission (FTC) enforces it.

Most of CAN-SPAM's stipulations only apply to commercial emails, as opposed to transactional emails.

What do I need to know about complying with CAN-SPAM?

In the United States, commercial email senders must be compliant with the CAN-SPAM Act; if they are not, they can receive tough penalties.

Here are some main CAN-SPAM's requirements for commercial emails:

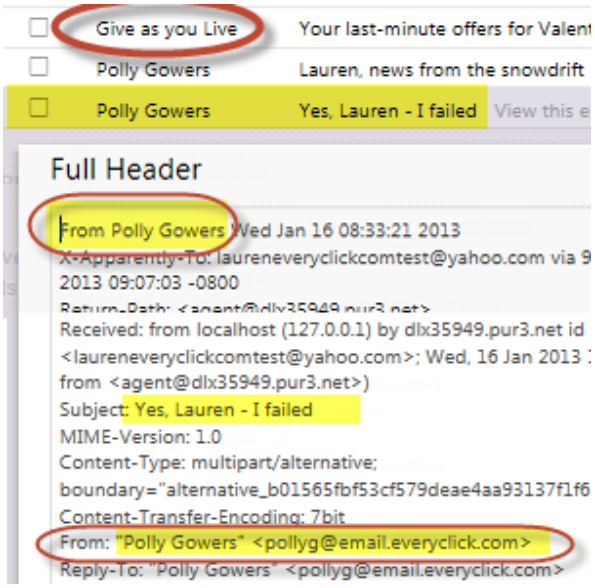
- Include a visible and working unsubscribe mechanism in all emails
- Include the List Unsubscribe header as specified under RFC 2368
- Honor unsubscribe requests within 10 days
- Do not sell, share, or lease the emails of customers who opt-out
- For unsubscribe functionality, follow all United States CAN-SPAM standards

Here is the main CAN-SPAM requirement for commercial *and* transactional emails:

- Do not include false or misleading header information

Examples of acceptable and misleading headers

Example of an acceptable header



Example of a misleading header

What is the difference between commercial and transactional email?

Commercial messages sell or promote something or they solicit information. Transactional messages communicate about in-process transactions, deliver previously agreed-upon goods or services, or notify the recipient of a change to their account.

Transactional emails may include commercial content and still retain transactional status under CAN-SPAM if transactional content appears before commercial content and the subject line reflects only the transactional nature of the email.

Are there other laws regulating email?

Most states and countries have different laws for regulating email. Here are a few of the requirements you should be aware of:

- CalOPPA (California): Among other requirements, CalOPPA demands that senders post an easy-to-find privacy policy on their company website. The privacy policy must tell consumers what information the site gathers and what they'll do with it.
- Georgia SLAM SPAM E-Mail Act (Georgia): Among other stipulations, GA SLAM SPAM requires sender header and router information to be truthful and accurate. For more about truthful, accurate headers, click here.

- CASL (Canada): Among other requirements, CASL demands that senders provide an explicit opt-in from subscribers unless they have a prior business relationship.
- DPEC (Europe): Among other stipulations, the Directive on Privacy and Electronic Communications also demands that senders provide an explicit opt-in from subscribers unless they have a prior business relationship.

For a full list of United States laws for regulating email, click here. For a full list of laws regulating email worldwide, click here.

Role Accounts

What are role accounts?

Role accounts, such as postmaster@ and abuse@, are email addresses that customers, mailbox providers, and others can use to ask you questions, report abuse, or send notifications. The internet standard addresses for these accounts are postmaster@[yourdomain] and abuse@[yourdomain].

These accounts should be monitored by email administrators in your company who can respond quickly to fix any problems.

All sending domains referenced in email sent over Return Path Certified IP Addresses must have role accounts.

Why do I need role accounts for all domains appearing in my message headers?

Role accounts are one of the most important internet-standard methods used by our partner mailbox providers to ask questions, report abuse, or send notifications to Certified senders. To facilitate communications with our mailbox providers, Certified senders must have role accounts.

How do I best create and manage role accounts?

Here are some suggestions for how to best create and manage your role accounts:

- Respond to inquiries or complaints within 24 to 48 hours
- Don’t configure these accounts with anti-virus protection, anti-spam, or other software that might block messages
- Post these addresses in your WhoIS record

For more about role accounts, and their purposes, click here.

Authentication

Authentication technology (such as DKIM, SPF, and DMARC) allows mailbox providers to confirm your sending identity. Without authentication, your chances of being filtered or blocked is greatly increased. Certified senders need to have SPF in place for their Certified IPs.

SPF

What is an SPF record?

Sender Policy Framework (SPF) is an authentication protocol that links sending domains to sending IPs. This helps computers recognize the difference between forged and legitimate email. Used in tandem with DKIM (not required for Certification) and DMARC (also not required), SPF plays a key role in combating fraud.

Why do I need an SPF record?

SPF gives you the ability to better confirm that your email is legitimate. Because almost all major receivers check SPF natively or through third-party services, they may think your legitimate messages are fraud if you don't authenticate with SPF and other protocols.

To be compliant with Certification standards, you must publish an SPF record for all domains sending mail from Certified IPs.

How do I set up an SPF record for my Certified IPs?

Here is how you set up an SPF record:

1. Determine the domains and IP addresses you send from.
2. Generate an SPF record using a tool such as SPF Wizard. To remain compliant with standards, do not use PTR, ?all, or +all directives.
3. Copy the SPF record from the wizard and publish it to your DNS as a TXT record.
4. Check the validity of your record using a tool such as Kitterman.

Disclosure

Give your subscribers a clear appreciation and understanding of how you will use their email addresses.

Clear, Conspicuous Disclosure

What is clear, conspicuous disclosure?

Clear and conspicuous disclosure is the act of telling people (who are about to sign up for your email) what type of mail they will be receiving from you, how you got their email, and how their email and/or personal information will be used.

Why do I need to offer clear, conspicuous disclosure?

If users know what type of mail they'll receive, how you got their email, and how their email and/or personal information will be used, they will have a better experience with your mailing program and be less likely to complain about your email. This, in turn, affects your mailing — and brand — reputation for the better.

Also, CA OPPA and other laws regulating email require clear, conspicuous disclosure.

How do I offer clear, conspicuous disclosure?

At the point of collection, tell users (in plain, everyday language):

- What type of commercial or promotional email they will get from you
- Why their email address is being collected
- How you will share or rent their email addresses and/or personal Information
- Any consequences of sharing or renting their email addresses and/or personal information
- If you have gotten their email address through a relationship with another list owner
- The same thing you told them in the privacy policy (this is not required, but is a best practice)

Examples of acceptable and unacceptable notices of advertisements

Example of an email message with acceptable communication about the fact that it is an advertisement

Example of an email message with unacceptable notice that it is an advertisement

Consent

Mail to subscribers who want your mail — and, let people out if they don't want your mail anymore.

Opt-In

What is opt-in or consent?

Certified senders only send mail to people who want it. To make sure you're doing this:

- Only gather subscribers who opt-in through acceptable forms of consent
- Tell users what email they will get from you and what you'll do with their email addresses through a privacy policy and a clear and conspicuous disclosure statement
- Upon request, be able to provide proof of consent, including the date, time, originating IP address, and location (e.g., a URL) where you collected the address

What does it mean to opt in?

To opt in is, simply, to choose to be a part of something. If a user opts in to be on an email list, they have actively chosen to be on it.

Why do I need to allow users to opt in?

Successful email marketers get permission to send emails to their subscribers and potential customers. When subscribers are not expecting your emails, complaints increase, response rates suffer, and deliverability rates drop.

Also, though CAN-SPAM allows senders to legally send mail to recipients who have not opted in, other regulations do not. Make sure you send mail legally by allowing users to opt in.

What are acceptable forms of opt-in or consent?

Below, find a list of the four acceptable forms of consent. In each of these situations, senders must clearly state that the emails sent will be commercial and provide unsubscribe mechanisms.

Acceptable forms of consent:

- Confirmed Opt-In*:* In this situation, subscribers take a single step to confirm their subscription, such as selecting a checkbox.
- Double Opt-in: In this situation, the recipient receives a confirmation email once they opt-in. This helps you make sure everyone on your list actually wants your mail (and did not accidentally sign up, feel pressured into signing up, or change their mind). This action helps decrease the possibility of anyone being on your list who does not want to be.
- Pre-Selected Opt-in: In this situation, you pre-select users to receive your promotional emails by checking a box clearly stating this. By leaving the checked box intact, users consent to receive your email. This option is not foolproof, as not all users will notice the checkbox. This practice is not permitted for co-registration.
- Pre-Selected Opt-in with Verification: This practice sends a confirmation email to any recipients who have left the pre-selected opt-in checkbox intact. This action helps decrease the possibility of anyone being on your list who doesn't want to be.
- Co-Registration: This practice gives users the option to sign up and receive mail from a third party. Co-registration is acceptable only if acceptable forms of consent and disclosure are present and if the subscriber is only signed up to one list. Use co-registration with caution; it can be confusing to recipients if they did not remember leaving boxes checked and, in effect, accidentally signed up for emails they did not expect.

Even though these forms of consent are acceptable, subscribers may still complain if they accidentally opted in to receive email they didn't want. Always make sure subscribers are fully aware of all the commercial email they will receive — and who will be sending it.

What are unacceptable forms of gathering emails?

Certified senders must only send mail to users who have opted in to receive it. Some unacceptable modes of gathering emails are:

- **Renting, harvesting, or purchasing lists:** These modes of gathering email do not involve gaining active consent from recipients; therefore, they are not allowed.
- **Co-registration:** This practice is *unacceptable only if* the sender uses one check box to sign up users to multiple third-party email lists. Recipients must be able to opt in to one list at a time, as well as manage all parties they want to receive email from.

Forward-to-a-Friend (FTAF)

Otherwise known as peer-initiated communication, FTAF emails are those forwarded from a subscriber on your list to a contact not on your list.

What do I need to know about consent for FTAF emails?

FTAF messages must follow the same rules as regular email messages — and a few more — because they were sent without the recipient's consent.

For FTAF messages, make sure you comply with the acceptable forms of consent — as well as these opt-in rules:

- If a recipient of a FTAF email does not respond, you can only send *one* follow-up message — and no others
- Though you can place the name of the friend in the From line of the FTAF email, the Return-Path and Mail From domains must be your own
- For FTAF emails, you must provide users the ability to globally unsubscribe

Unsubscribe

An unsubscribe mechanism is, simply, a way for users to opt out of receiving your emails. This can be a link to a website, a response to an email, or a phone call.

Why do I need an unsubscribe mechanism?

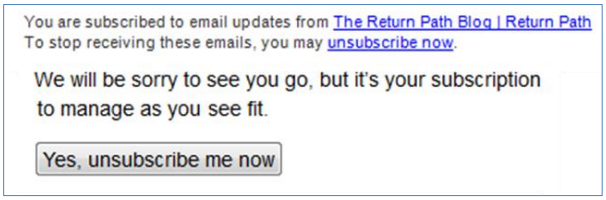
To be CAN-SPAM compliant, all promotional or commercial email must have unsubscribe functionality. It also must be clear, straightforward, and easy. Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.

Also, if you make it hard for people to unsubscribe from your email, their only other choice is to complain by hitting "This is Spam."

What do I need to know about unsubscribe mechanisms?

For Certified senders, all unsubscribe mechanisms need to be:

- Easy-to-use:
  - Make sure your unsubscribe mechanism is easy to find
  - Make sure it's easy for users to understand how to unsubscribe
  - Don't require users to log into their account in order to unsubscribe



Here is an example of an easy-to-use unsubscribe mechanism

- Timely:
  - Respond to requests within 3 days
  - Resolve requests within 10 days

- Persistent:
  - Once a user has opted out, don't send them commercial or promotional emails
  - Once a user has opted out, don't sell, share, or lease their addresses or information

- Indefinite:
  - Keep the unsubscribe link alive for at least 60 days following the sending of the commercial message
  - Do not contact users or add them back into your email list unless they opt in again

- Absolute:
  - Allow the recipients of peer-initiated mail to globally unsubscribe or opt out of *all* of your emails

Here is an example of a global unsubscribe process

- Flexible:
  - Let users unsubscribe through alternative methods, such as phone calls, postal mail, and email accounts that don't usually deal with unsubscribe requests

- CAN-SPAM-compliant (from the actions listed above, these listed below are necessary for CAN-SPAM compliance):
    - Handle unsubscribe requests within 10 days
    - Don’t make the recipient take any step other than sending a reply email or visiting a single page on an Internet website
    - Make sure all peer-initiated emails offer the ability for users to unsubscribe from all future mailings

Security

Take adequate, industry-standard steps to keep your database and systems secure so you can protect your infrastructure and your subscribers.

Secure Systems

Why do I need a secure system?

A secure system prevents malware — such as viruses, worms, spyware, adware, trojans, recursive DNS, etc. — to infiltrate your infrastructure, and it prevents open proxies or open relays that would allow unauthorized content to be sent from your Certified IPs.

How do I maintain a secure system?

To be compliant with systems security requirements, Certified senders must:

- Not have open relays or open proxies
- Have a valid rDNS record
- Have a fully qualified DNS record (FQDN)
- Have consistent HELO server names
- Have a fully-qualified DNS record with a Fully Qualified DN
- Maintain IP groups with no more than three discreet netblocks
- Have an SPF record

What is an open relay?

An open relay is an SMTP server configured so that anyone can send mail through it.

Why can’t I have an open relay?

If you have an open relay, spammers could use it to send mail — which could result in you getting blacklisted.

How do I avoid open relays?

Configure your SMTP server so that the mail relay parameter only sends mail from known domains or IPs — and only allows access to someone with a username and password.

By default, relays are sometimes set to open. Check to see if you have an open relay at DNS Goodies or MX Toolbox.

What Is an open proxy?

An open proxy is a forwarding proxy server anyone on the Internet can use.

Why can't I have an open proxy?

Open proxies do not filter, encrypt, or otherwise check what content is coming into servers. Because of this, they can allow malware to be downloaded and infect computers.

How do I avoid open proxies?

Open the preference center in your browser and make sure the proxy is not set to open.

What is reverse DNS (rDNS)?

rDNS is a protocol used to translate the sending server IP address into its hostname (host.example.com).

During a reverse DNS lookup, your SMTP server verifies that the sender's IP address matches the domain name submitted by their SMTP client in the HELO command.

Why do I need a valid rDNS record?

Proper rDNS configuration is an essential best practice and an important form of authentication. Also, by proving that your IP is sending for domains you own, a valued rDNS record provides transparency for your subscribers.

What is a fully qualified DNS record (FQDN)?

A fully qualified DNS record specifies both the local hostname and the parent domain name.

For example, if the local hostname was 'host' and the parent domain name was 'domain,' a fully qualified DNS record check would return host.domain.com.

What is a valid rDNS record with a fully qualified domain name?

Fully qualified DNS records specify both the local hostname and the parent domain name (host.domain.com); therefore, when an rDNS is performed, the IP returns both the hostname and parent domain name.

Why do I need a valid rDNS record with a fully qualified domain name?

By having a valid rDNS record with an FQDN, you prove that your IP address is using sending domains you own.

Without a valid rDNS record with a FQDN, spammers may be able to send mail from your servers. Also, blacklists may list your IPs because they believe your rDNS to be unassigned or dynamic.

What is HELO?

In the SMTP conversation (the conversation between sending and receiving servers when an email is being sent), the HELO identity names the sending IP's FQDN or its complete domain name.

Why do I need a consistent HELO server name that matches the rDNS of the sending IP address?

Certified senders' HELO identity must be in the form of a domain name that matches the rDNS of the sending IP address.

Having a consistent HELO identity that matches the sending IP's rDNS helps close the circle authenticating that senders' servers are only sending mail they own.

What are netblocks?

A netblock is a range of consecutive IP addresses — for instance, 196.25.0.0-196.25.255.255 or 196.25.0.0/16.

Unless specified in writing by Return Path, Certified senders should have IP groups that span no more than three separate netblocks.

Why can't my IP groups span more than three netblocks?

Unless your company has extensive operational needs, Certified senders should only need one or two IP groups. Sending from a large number of IPs makes it appear as if you are trying to water down or avoid bad reputation metrics. Also, it is easier for senders to maintain a good IP reputation with fewer IP addresses.

Therefore, Certified senders cannot have more than two IP groups when they are accepted into the program. They also can't add so many new IPs after they are Certified that they exceed this threshold.

Secure Databases

What is a secure database?

A secure database prevents others from tampering with your recipients' email addresses and related personal information.

Why do I need a secure database?

Secure data systems protect your email program and your subscriber data. Data breaches appear in headlines every day; protecting your users' information should be a priority.

Performance

Remain within Certification compliance metrics by following industry best practices for complaints, unknown users, spam traps, and blacklistings.

What is good performance?

Senders with good performance are those who stay within the stated thresholds, which include metrics for:

- Complaints
- Spam traps
- Unknown users
- Blacklists
- Sender Reputation Data (SRD)

We expect you as a Certified sender to stay within the thresholds most of the time across most of your IPs.

Compliance thresholds for IP Certification

Individual IP Microsoft SRD compliance thresholds			
SRD Volume	0-4	5-10	11 or more
SRD Rate Threshold	Not enforced	5 Junk Votes	45%

Microsoft Group SRD compliance thresholds				
Group SRD Junk Votes	0-9	10-30	31-50	51 or more
Group SRD Rate Threshold	Not enforced	75%	65%	55%

Note: We enforce the Group SRD standard if you have 2 or more Certified IPs.

Complaint, Trap, and Blacklist compliance thresholds	
Microsoft: Complaint Rate Threshold (30 day average)	All sending volumes 0.2%
Yahoo!: Inbox Complaint Rate Threshold (30 day average)	All sending volumes 0.6%
AOL: Overall Complaint Rate Threshold (30 day average)	All sending volumes 0.3%
Comcast: Complaint Rate Threshold (30 day average)	All sending volumes 0.3%
Spam Trap Thresholds (30 day cumulative)	3 Critical Trap Hits 5 Significant Trap Hits
RP Trap Network 1 Threshold (30 day cumulative)	100 Trap Hits
Cloudmark Trap Threshold (30 day cumulative)	100 Trap Hits
Cloudmark Complaint Rate Threshold (30 day cumulative)	1.0%
Blacklist Thresholds (current listing)	1 Critical Listing 2 Significant Listings

Note: Certification only enforces on its mailbox provider complaint rate thresholds if you receive a set minimum number of complaints.

Here is the list of mailbox providers and the minimum number of complaints you need to receive in order for Certification to enforce its complaint rate thresholds:

- Microsoft: 200 complaints
- Yahoo!: 200 complaints
- AOL: 100 complaints
- Comcast: 100 complaints

Why do I need to maintain good performance?

Repeat or prolonged non-compliance shows that you may have picked up some email acquisition, hygiene, or security practices that are not up to Certification standards.

If you repeatedly fall out of compliance — or remain out of compliance for a long time — your sending practices may be subject for review, and your IPs may be subject to probation or removal from the Certification program.

How do I maintain my good performance?

To remain compliant, maintain good performance standards by monitoring data, such as feedback loops, or reviewing email best practices provided by your account manager, or found in the Help Center or on returnpath.com.

Also, to help with engagement monitoring, bounce processing, list suppression, and traffic segmentation, you must use a bulk mailing program or software for commercial emails.

Domain Certification Program Addendum

This addendum lists all standards and requirements specific to Domain Certification. To qualify for Domain Certification, senders must authenticate their domains with DKIM.

In addition, senders must meet all of the applicable Certification standards and requirements outlined on pages 1 through 25. They must also remain within the thresholds for Domain Certification compliance metrics which are included below.

Authentication

What is DKIM authentication?

DomainKeys Identified Mail (DKIM) is a protocol that allows an organization to transmit a message in a way that allows mailbox providers to verify who the sender is through cryptographic authentication. When a message has been signed using DKIM, mailbox providers who successfully validate the signature can use information about the signer as part of a program to limit spam, spoofing, and phishing, although DKIM does not tell mailbox providers to take a specific action.

Depending on the implementation, DKIM can also help ensure that the message has not been modified or tampered with in transit, allowing Return Path Certification to associate volume and complaints with the correct domain.

Why am I required to send from a domain using DKIM authentication?

Mailbox providers base sending reputation either on IP address or domain traffic. You can only control your reputation and status in the Domain Certification program by sending from domains that are authenticated with DKIM.

If you do not, the metrics that the Certification program monitors will not accurately reflect your company's sending reputation. So, you cannot share traffic on Certified IP addresses or domains — even with organizations you have a relationship with.

How do I set up DKIM for my sending domains?

1. Determine all the domains that you send from.

2. Install and configure DKIM on your email server.

   All outgoing email must be signed, meaning that you need to install a DKIM package specifically for your email service. To determine whether your platform has DKIM software, you can check the DKIM.org site or check with your vendor. If you use an email service provider, work with them to set up the DKIM record.

3. Create a public and private DKIM key pair.

Generate an DKIM record using a tool as the DKIM Wizard from port25.

Recommendations:

- Make the selector name descriptive of the type of email you are sending, such as **marketing** or **newsletter**.
- Standardize your selector names for ease of tracking.
- Ensure your key is 1024-bit or higher

4. Publish your public key.

   Store your public key in the TXT portion of the domain that you are authenticating.

5. Store your private key.

   Your private key is also generated by the wizard and needs to be stored where your DKIM package specifies.

6. Configure your email server.

7. Test the system.

   Send an email from your email server to checkmyauth@auth.returnpath.net. You will receive an email indicating whether DKIM passed or failed, as well as a warning if your key is not strong enough.

Performance

Compliance thresholds for Domain Certification

We expect you as a Certified sender to stay within the thresholds most of the time across most of your domains.

Microsft SRD compliance threshold	
Microsoft: SRD Rate Threshold (30 day average)	50% with 5 Junk Votes

Complaint, Trap, and Blacklist compliance thresholds	
Microsoft: Complaint Rate Threshold (30 day average)	All sending volumes 0.4%

Comcast: Complaint Rate Threshold (30 day average)	All sending volumes 0.3%
Spam Trap Thresholds (30 day cumulative)	3 Critical Trap Hits 5 Significant Trap Hits
Blacklist Thresholds (Current listing)	1 Critical Listing 2 Significant Listings

Microsoft Sender Reputation Data (SRD) in Domain Certification

The SRD rate for Certified domains is calculated using the following formula across all of your IPs:

Microsoft SRD Rate = sum of junk votes / sum of total votes

All domains in your program will be suspended if the SRD rate is 50% or higher AND you have 5 or more junk votes.