Return Path

Certification Requirements

We Know Email

returnpath.com

All requirements effective July 16, 2018

Table of Contents

Introducing Certification
- Become Certified
- Stay Certified

Certification requirements overview
- Breaking down the requirements

Part 1: Business Model

Part 2: Measurability

Part 3: Infrastructure

Part 4: Email message content

Part 5: Points of collection

Part 6: Consent
- Examples of prohibited consent practices

Part 7: Privacy policy

Part 8: Legality

Part 9: Security

Part 10: Feedback loops (FBLs)

Part 11: Communication

Part 12: Performance and compliance

Need help?

Introducing Certification

Return Path Certification is the industry's most unique and powerful whitelist. But it's also much more than that. It's a program that provides the exclusive data and mailbox provider benefits you need to get more email delivered, reach more subscribers, and increase revenue.

Become Certified

Our Certification program is designed for best-in-class senders that meet top mailbox providers' and subscribers' expectations, and follow industry-standard best practices. Throughout your process to become Certified, we will work together to ensure your program fulfills our program requirements.

Here are the key steps to becoming Certified:

1. Submit this form if you're interested in Certification and have not been in contact with Return Path. If you're already a Return Path client, reach out to your account representative or submit a ticket.
2. At the beginning of the Certification process, we conduct a comprehensive audit of your email program to ensure it meets all of the requirements detailed below.
3. During the audit, we will notify you if any parts of your email program do not meet our requirements. In order to continue the audit, you will need to complete any updates within 30 days of our request. (Don't worry, we'll provide you with additional information on the changes and how to complete them.)
4. Once you make the appropriate changes, we finalize your audit and send you an account activation email.
5. After becoming Certified, your IPs will begin receiving benefits at AOL, Microsoft, Yahoo!, and other global mailbox and email security providers.

Stay Certified

As a Certified sender, you're required to consistently meet the Certification requirements used to evaluate your program during the audit. Meeting the requirements on a consistent basis ensures you receive the program's full deliverability benefits. We conduct periodic wellness checks to ensure your email program is still meeting our requirements and protect the Certification program.

While you're Certified, you'll receive benefits such as:

- A measurable inbox placement increase at mailbox providers like Microsoft, Yahoo!, AOL, and more, including during the crucial holiday season when mailbox providers often throttle and filter high-volume senders.

- Exclusive data feeds from mailbox providers delivering detailed information about your KPIs, placement, and Certification performance.
- A compliance team dedicated to 24/7 monitoring, providing you with security alerts and working with you through the resolution of any compromises.

We understand that issues happen and you may fall out of compliance once in a while, which may result in a temporary suspension from the program while you get back on track. However, if you excessively, repeatedly, or egregiously violate the requirements, we will notify you and work with you to make any necessary update. We also reserve the right to remove you from the program if necessary.

Certification requirements overview

Now that you have learned about the Certification program and how to become and stay Certified, it's time to learn about our Certification requirements. The information listed below describes the requirements your email program must meet to complete the initial audit and remain Certified once you are accepted into the program.

Breaking down the requirements

The Certification requirements are divided into 12 different parts of your email program, such as your infrastructure or privacy policy. Altogether they create a complete view of your email program and determine if you are eligible for our Certification program.

Here are the different parts we check and what they mean:

- **Business Model** explains who you are and what you do
- **Measurability** illustrates how much and how often you send email
- **Infrastructure** shows how you send, authenticate, and manage email
- **Email Message Content** is how you present yourself to your subscribers
- **Points of collection** is how you gather email addresses
- **Consent** explains how subscribers agree to receiving your email
- **Privacy policy** documents all the details of your email program
- **Legality** is important to your business and you adhere to any applicable spam and data privacy laws that impact you and your subscribers
- **Security** showcases how you take care of your systems and subscribers' data
- **Communication** indicates your willingness and ability to communicate with Return Path
- **Feedback loops (FBLs)** usage shows that you care about keeping a clean, healthy list of subscribers
- **Performance and compliance** demonstrates if your email program is able to stay within thresholds established by mailbox providers and subscribers

Read on for details about each section listed above.

Part 1: Business Model

To begin your Certification audit, we review your **business model**. Your business model gives us important information about your overall email program and helps us determine if you're a good fit for Certification.

Here are the requirements your business model must meet to become and stay Certified:

1. **Business registration**

    a. Your business is verifiable by a third-party source through a legitimate online website, such as a country registry, or an application such as Dun & Bradstreet.
    b. Your business registration includes your business's current physical address.
    c. Your business has been operational for at least one year.
    d. Your business does not use a registered agent to obscure any of your business's information.

2. **Website presence**

    a. Your business maintains valid website and landing pages for all brands whose marketing email will be sent over Certified IPs for at least the past 6 months.

3. **IP addresses and content**

    a. We currently only Certify dedicated IPs. Shared IP addresses are not eligible.
    b. Certified IPs can only send first-party email. This means Certified IPs cannot send third-party email, which is email sent on the behalf of others that are not your brand.
    c. Certified IPs can only send transactional and commercial email. This means you cannot use Certified IPs to send corporate email, which often includes internal communications between co-workers or customer support emails.
    d. Certified IPs must send templated, clearly branded emails. They cannot send free-form content such as web forms or open text boxes.

IMPORTANT: We will not Certify IP addresses if your business fits into one of the following categories:

- Agencies
- Third party mailers
- Lead generation
- Penny bid model websites
- Illegal activities
- Human trafficking

Part 2: Measurability

If your business model meets our requirements, we review your email program's **measurability**. Measurability helps us understand your overall sending patterns, including how often you're sending to your subscribers.

Here are the measurability requirements you must meet to become and stay Certified:

1. **Measurable and consistent volume**

    a. Your IP address sends at least 100 email messages to each Microsoft and Yahoo! over the most recent 30-day period, as seen in Return Path's data sources.
    b. Your IP address maintains measurable and consistent volume to remain Certified. Consistency is determined based on your particular program and sending behavior. IP addresses without measurable and consistent volume are suspended after 30 days and deleted from the application process or program after 90 days.

2. **Targeting mailbox providers**

    a. Your business cannot use a single IP address to send email to one specific mailbox provider in the Return Path Consumer Network or Provider Network.
    *Occasional and temporary single-receiver mailings may be tolerated under certain circumstances but Return Path must approve it in writing.

Part 3: Infrastructure

Once your measurability meets our requirements, we review your email sending **infrastructure**. Infrastructure refers to the hardware and process used to deploy email. It's crucial that you send email from well-maintained infrastructure systems that uses best practices.

Keep in mind that you may need to work with your Email Service Provider (ESP) or internal IT team to comply with the requirements listed below in order to become and stay Certified:

1. **Dedicated IP addresses**

    a. Your business is the only entity sending email over dedicated IP addresses for at least 60 days.

2. **Open relays**

a. Your infrastructure does not have any open relay servers.

3. **FCrDNS**

   a. Your IP address reverse DNS (rDNS) entries matches the forward DNS entries, otherwise known as Forward-Confirmed reverse DNS (FCrDNS).

4. **Blacklists**

   a. Your IP addresses or domains are not on a Return Path-monitored blacklist. Repetitive or excessive blacklistings may result in the suspension or termination of your Certification benefits. Learn more about blacklist thresholds below

5. **SPF**

   a. All of your Mail From and Return-Path domains have published Sender Policy Framework (SPF) records. Learn how to set up SPF here
   b. Your SPF records pass mailbox provider authentication checks within reasonable operational tolerance as determined by Return Path.
   c. All sending and Return-Path domains do not use a `+all` or `?all` directive.
   d. All sending and Return-Path domains do not include a pointer (PTR) record.

6. **DKIM**

   a. All of your email sent over Certified IPs have DomainKeys Identified Mail (DKIM) authentication configured. Learn how to set up DKIM here
   b. Your DKIM authentication passes mailbox provider authentication checks within reasonable operational tolerance as determined by Return Path.

7. **DMARC** (recommendation only)

   a. We *highly recommend* you implement Domain-based Message, Authentication, Reporting & Conformance (DMARC), however, it is not currently a Certification requirement. Learn how to set up a DMARC record here

8. **Role accounts**

   a. You configure and maintain abuse@ and postmaster@ role accounts for all sending and Return-Path domains to handle complaints and other issues.
   b. We also recommend you support and maintain other standard role accounts such as support@ or help@ accounts.

9. **WHOIS records**

   Your WHOIS records must meet the following criteria for all sending domains, Return-Path domains, and website domains associated with the email sent from your IP addresses.

   a. Your business maintains up-to-date WHOIS records.
   b. Your WHOIS records contain your business's registered name. For your Return-Path domain WHOIS records, the legal name can be your Email Service Provider (ESP) if applicable.
   c. Your WHOIS records list at least one method of contact such as phone number or email address.
   d. Your WHOIS records contains your business's current mailing address that is not a P.O. box.
   e. Your WHOIS record does not obscure your business's information by using proxy or privacy services.
   f. See an example and learn more about WHOIS records here

10. **List maintenance**

    a. Your business uses email address list maintenance systems to reliably receive and process delivery errors, bounce messages, and other replies from receiving networks.
    b. You process hard bounces from emails sent over your IP addresses by removing the undeliverable email address from all future mailings.

Part 4: Email message content

If your infrastructure passes our requirements, we review your **email message content**. We primarily ensure that your email follows best practices as described by mailbox providers. This includes being transparent with your subscribers about who you are.

Here are the email message content requirements you must meet to become and stay Certified:

1. **Branding**

   a. You send email that clearly uses your business's branding to accurately identify yourself to subscribers.

2. **Subject line**

   a. All subject lines are accurate.
   b. All subject lines clearly relate to the email body content without being deceptive or misleading.

c. No subject lines include “RE:” or “FWD:”. Using these abbreviations is typically seen as a deceptive tactic prompting subscribers to open the email as if it were sent from an individual rather than a commercial sender.

3. **Email body content**

   a. All email body content is truthful and accurate.
   b. For any commercial, promotional or transactional mail, you must include your business’s valid physical mailing address.
   c. You do not use URL shorteners in your body content. This includes, but is not limited to, the use of Bitly, TinyURL, and Google URL Shortener.
   d. You cannot use a Report Spam link within your email body’s content. This is typically used by senders who attempt to avoid mailbox provider complaints.

4. **Message headers**

   a. Email message headers are not falsified, obscured, deceptive, or misleading in any way. Examples include the Return-Path header, the From header, the Friendly From name and address, and more.

5. **Third-party content**

   As listed above in Part 1, first-party email that contains third-party content (such as ad sponsored content) is eligible for Certification but must meet the following requirements:

   a. The subject line references the first-party content.
   b. All email messages are clearly and conspicuously branded as coming from you, the Certified sender.
   c. The majority of the email’s content is your business’s marketing, including links and logos.
   d. The From and Friendly From address identifies the Certified sender and does not include the third party’s name.

6. **Unsubscribe process**

   a. Every commercial, promotional, or peer-initiated email sent over your IP address includes a list-unsubscribe header and an unsubscribe link.
   b. Unsubscribe instructions are clear, conspicuous, and easily understood.
   c. Unsubscribe mechanisms are easy for the recipient to use when unsubscribing from your email program. User-friendly unsubscribe mechanisms include replying to the commercial or promotional email with the request or selecting a link to unsubscribe through an online process.

d. The unsubscribe process does not require a recipient to provide any information other than their email address. We recommend using a one-click process such as selecting a link.
e. Once a recipient unsubscribes from your email program, you will no longer send them any commercial or promotional email. Additionally, you will not sell, lease or share the recipient's email address or personal information to any third party.
f. You process and fulfill all unsubscribe requests within 3 days of receiving the request.
g. You honor anyone's request to unsubscribe from your email program indefinitely regardless if it was peer-initiated. Or, until they opt into your program again. Learn about Certification's opt in requirements here
h. Unsubscribe links that are sent through any email remain active and functional for at least 60 days following the date it was sent.
i. If any recipient requests to unsubscribe from your email program through non-standard unsubscribe mechanisms, you still process the request in a timely manner. Examples of non-standard unsubscribe mechanisms include postal mail, alias email addresses, postmaster or abuse addresses, and telephone calls.
j. You must include a valid unsubscribe link in any email survey requesting feedback from recipients. However, you do not need to include an unsubscribe mechanism if you send a recipient a survey related to a previous transaction that occurred between your business and the recipient.

Part 5: Points of collection

Once we determine your email message content and unsubscribe processes meet our requirements we review how you collect email addresses, otherwise known as your **points of collection**. It's critical that you directly tell subscribers about the type of email they're signing up for, what they should expect, and more.

Your points of collections must meet the following requirements:

1. **Clear and simple**

a. You have clear and simple disclosure at all points of collection. Including a link to your privacy policy instead of listing the information does not fulfill this requirement.
b. You disclose information to the subscriber about the email they will receive when they enter and submit their email address. This could include an accurate definition of the content and frequency.
c. You must clearly disclose if you share or rent your subscribers' email addresses or any other related personal information, at all points of collection.

2. **Privacy policy**

a. Your privacy policy is clearly, conspicuously, and directly referenced at all points of collection, including mobile applications. Learn more about our privacy policy requirements here

Part 6: Consent

If your points of collection pass our requirements, we review your **consent** practices. We want to know that you properly ask for and receive consent from your subscribers in accordance with these requirements.

Here are the consent requirements you must meet to become and stay Certified:

1. **Acceptable opt-in methods**

   You must use one of the following opt-in methods when acquiring consent from subscribers:

   a. **Confirmed (double) Opt-in**: After a subscriber opts into your email program, you must send them an email verification for them to confirm their subscription. The subscriber must activate the URL provided in the email to confirm their subscription before you send any additional emails.
   b. **Opt-in with notification**: After a recipient opts into your email program, you must send them an email notification affirming their subscription and provide them with clear unsubscribe instructions, before you send any additional emails.

   For **Confirmed Opt In** and **Opt In with Notification** you may have a pre-selected checkbox that users can deselect upon account creation to opt out of promotional emails.

   c. Other Consent Methods: If your email program is relying on an alternative consent method as your legal basis for processing of personal data, you will need to provide us with documentation of that method, such as a completed legitimate interest assessment or other assessment.

   As a reminder, it is also important to review and comply with applicable laws and regulations that impact you, which may be greater than our Program Requirements.

2. **Co-registration**

   When you give users the additional option to sign up for third-party or affiliate email on your website, you must meet the following requirements. These requirements also apply to any brands that operate under the same parent company.

a. At the point of collection, you clearly and conspicuously name the business from which the recipient is also signing up to receive email.
b. You clearly define every brand a recipient may be signing up to receive email from. You also have separate sign-up options, such as de-selected checkboxes. This requirement also applies to brands that operate under the same parent company.
c. You are able to produce proof of consent where any addresses are collected. Proof of consent includes the date, time, originating IP address, and location (URL).

3. **Forward to a Friend and peer-initiated email**

a. The sign-up form includes CAPTCHA or reCAPTCHA to verify the legitimacy of the friend initiating the email. CAPTCHA and reCAPTCHA helps prevents bots or exploitative users.
b. You only send one Forward to a Friend commercial or promotional email to the submitted address.
c. If a Forward to a Friend email recipient does not respond, you can send only one follow-up email.
d. The Return-Path and Mail-From (MFrom) domains are your own domains listed in the email header.
e. You provide recipients with a way to unsubscribe from all future email, which is commonly referred to as a global unsubscribe.
f. Emails do not contain links or URLs to external web addresses.
g. Emails can include personalized comments up to 140 characters.
h. An individual user can only use this feature to send a maximum of 100 messages over a 24-hour period.
i. In order to send Forward to a Friend email recipients additional commercial or promotional email, they must opt into your email program use an acceptable opt-in method as listed above.

Examples of prohibited consent practices

- Pre-selected single opt-in (without notification)
- Single opt-in (without notification)
- List harvesting
- List rental, purchase, or email append
- Email prospecting

Part 7: Privacy policy

If your consent practices pass our requirements, we review your **privacy policy**. It's important to note that your privacy policies should adhere to any applicable laws. Beyond that, we ensure you're fully transparent with potential subscribers about your email program, how they can reach you, and what data you collect.

Here are the privacy policy requirements you must meet to become and stay Certified:

1. **Easily accessible**

    a. Your privacy policy is easily accessible on your website's homepage.

2. **Unsubscribe directions**

    a. Your privacy policy includes clear and direct directions that tell subscribers how they can unsubscribe from your email program.

3. **Physical address**

    a. Your privacy policy includes a physical address for your company and any partner companies. P.O. boxes are acceptable although subscribers prefer street addresses.

4. **Point of collection**

    a. Your privacy policy accurately reflects your business's practices when referenced at points of collection. For example, you must disclose how an email address is used after you collect it.

5. **Data disclosure**

    a. Your privacy policy must tell recipients about all personal information your business collects and how it might be shared.

6. **Brand ownership**

    a. If you are a parent company to multiple brands, you must include a list of every other brand you own in each privacy policy.
    b. If you are a brand owned by a parent company, you must include the name of the parent company in your privacy policy.

Part 8: Legality

As a business, it's important you adhere to any applicable **laws and regulations** that impact you. Each country and territory has legislation related to email and data practices. It's imperative that you fully comply and follow these laws and regulations wherever you operate.

Examples include but are not limited to:

- United States of America: Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM)
- Canada: Canada's Anti-Spam Legislation (CASL)
- European Union: GDPR (General Data Protection Regulation)
- Australia: Spam Act of 2003

Part 9: Security

Continuing with your audit, we review your **security practices**. It's important your business takes adequate, industry-standard steps to keep your database and systems secure so you can protect your infrastructure and your subscribers.

Here are the security requirements you must meet to become and stay Certified:

1. **Infrastructure**
    a. Your email infrastructure is maintained and operated in a responsible manner.
2. **Subscriber protection**
    a. Your business uses adequate, industry-standard policies and procedures to secure and protect your subscribers' email addresses and any other personally identifiable information (PII).
3. **Secure systems**
    a. Your business uses industry-standard efforts to prevent open proxies, open relays, computer viruses, worms, spyware, adware, trojans, recursive DNS, or any other item identified as malware on your infrastructure.
4. **Compromises**
    a. You will notify Return Path in writing within 2 business days if you discover your IP or domain has been compromised.
    b. If your IP or domain is ever compromised, you agree that the IP or domain will not be re-enabled in the Certification program until a Return Path employee completes a review and determines that the cause of the compromise has been properly mitigated.

Part 10: Feedback loops (FBLs)

As a best practice, we recommend you sign up for all available feedback loops (FBLs) in order to effectively manage and reduce complaints. A full list of FBLs can be found here.

If for some reason you aren't able to sign up for the entire list of FBLs, here are the feedback loops you must sign up for to become and stay Certified:

- Comcast IP and domain feedback loop
- Yahoo! Feedback loop
- Microsoft Junk Email Reporting Program
- AOL feedback loop

Part 11: Communication

Whether you are just beginning your Certification application or audit, or you're already Certified, it's important that there is clear and open communication between your business and Return Path.

Here are the communication requirements you must follow in order to become and stay Certified:

1. **Issue resolution**

    a. To resolve any Certification program-related issues, you and and any team involved in sending email will cooperate with the Certification administrators.
    b. You respond to any program notice within 3 days, and you begin taking any required actions within 10 days of the notice.

2. **Contact information**

    a. You maintain up-to-date contact information with Return Path.

Part 12: Performance and compliance

A large part of staying Certified on a regular and consistent basis is making sure your email program stays within our performance thresholds. When you remain within the thresholds listed below, you receive benefits at the corresponding mailbox providers, improving your overall deliverability to ultimately reach more of your subscribers.

Note: We actively work with our partners to determine thresholds and suspensions.

You must meet the following performance requirements in order to become and stay Certified:

Individual IP Microsoft SRD compliance thresholds

SRD Volume	0-4	5-10	11 or more
SRD Rate	Not enforced	5 Junk Votes	45%

Microsoft Group SRD compliance thresholds

SRD Volume	0-9	10-30	31-50	51 or more
SRD Rate	Not enforced	75%	65%	55%

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

Tip: Having problems with your Microsoft SRD rates? Check out these resources.

Complaint, trap, and blacklist compliance thresholds

Microsoft: Complaint Rate (30-day average)	All sending volumes 0.2%
Yahoo!: Inbox Complaint Rate (30-day average)	All sending volumes 0.6%
AOL: Complaint Rate (30-day average)	No longer enforced*
Comcast: Complaint Rate (30-day average)	All sending volumes 0.3%
Spam Traps (30-day cumulative)	3 Critical Trap Hits 5 Significant Trap Hits
RP Trap Network 1 (30-day cumulative)	100 Trap Hits
Cloudmark Traps (30-day cumulative)	100 Trap Hits
Cloudmark Complaint Rate (30-day average)	All sending volumes 1.0%
Blacklists (Current listing)	1 Critical Listing 2 Significant Listings

***Return Path stopped enforcing compliance for AOL on 1/18/19 due to Oath migration, or the consolidation of Yahoo and AOL infrastructures. AOL data will still appear in the Certification user interface and DPR though AOL data will decrease over time until there is no AOL-specific data left to report. You will notice a steady decrease in AOL data alongside a steady increase in Yahoo data. For more information on the migration, click here.**

Note: Certification only enforces mailbox provider complaint rate thresholds if you receive a minimum number of complaints at specific mailbox providers:

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

Need help?

For additional insight into Certification and its requirements, or to learn how to troubleshoot deliverability and reputation issues, visit our Help Center.