Certification Requirements

Return Path
FROM VALIDITY

Table of Contents

Introducing Certification

Return Path Certification is the industry's most powerful whitelisting and sending practices program, but it's also much more than that. It's a unique program that combines exclusive data and insight into your inbox placement with benefits directly from mailbox providers to get more emails 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. At the beginning of the Certification process, we conduct a comprehensive audit of your email program to ensure it meets all the requirements detailed below.
2. During the audit, we will notify you if any parts of your email program do not meet our requirements and provide you with additional information on the changes and how to complete them. In order to continue the audit, you will need to complete any updates within 30 days of our request.
3. Once you make the appropriate changes, we finalize your audit and send you an account activation email.
4. 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. Periodic wellness checks are conducted to protect the Certification program and to ensure your email program is still meeting our requirements.

- A measurable inbox placement increase at mailbox providers like Microsoft, Yahoo!, 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

To become and stay Certified, you will need to meet the requirements of the Certification program. These requirements are based on best practice guidance established in partnership with our mailbox provider partners.

Breaking Down the Requirements

- **Business Model:** be transparent about who you are and what you do
- **Measurability:** send email in volumes and at frequencies that appeal to your subscribers
- **Infrastructure:** properly send, authenticate, and manage email
- **Email Message Content:** present yourself distinctly and accurately to your subscribers
- **Disclosure:** inform subscribers that you're collecting their email address
- **Consent:** explain how subscribers agree to receiving your email
- **Privacy policy:** document all the details of your email program
- **Legality:** adhere to any applicable spam and data privacy laws that impact you and your subscribers
- **Security:** show how you take care of your systems and subscribers' data
- **Communication:** communicate clearly and openly with Return Path
- **Feedback loops (FBLs):** use feedback to keep a clean, healthy list of subscribers
- **Performance and Compliance:** demonstrate your email program stays within thresholds established by mailbox providers and subscribers

Part 1: 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
    - Your business is verifiable by a public third-party source through a legitimate online website, such as a country registry, or an application such as Dun & Bradstreet.
    - Your business registration includes your business's current physical address.
    - Your business has been operational and legally registered for at least one year.
    - Your business does not use a registered agent to obscure any of your business's information.
2. Website
    - 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.
    - Your website(s) utilize Hypertext Transfer Protocol Secure (HTTPS).
3. IP addresses and content
    - We currently only certify dedicated IPs. Shared IP addresses are not eligible.
    - 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. email. This means you cannot use Certified IPs to send corporate email, which often includes internal communications between co-workers or customer support emails.
    - 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:

Email Services Providers	A sender mailing on behalf of brands that are not owned by the Certified entity. Including, but not limited to, Email Service Providers, Brand Licensing, Publishers, White-Labels, etc.
Agencies	Companies that do not fully own the brands that they are supporting or servicing. For example, companies that develop creative and marketing strategies on behalf of others.

Third Party / Affiliate Mailers	Companies that send other brands' content to their own email list for a fee. Companies that include content that are related to a third party is allowed at Return Path's discretion.
Lead Generation	Companies that collect email addresses for the purpose of growing sales pipeline, prospecting, etc. for brands that are not fully owned by the Certified entity.
List Rental Providers	Companies that compile permission-based email lists and sell access to them for brands to send email marketing campaigns to.
Penny Bid Auction	Online retailers that offer one cent bidding to their customers.
Illegal Activities	Business operations or practices that may violate the la in a given jurisdiction.
Human Trafficking	Businesses operating for the purpose of illegally transporting people from one area to another.

Part 2: Measurability

1. Measurable and consistent volume
    - 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.
    - 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 not eligible for review.
    - Once Certified, IP addresses without measurable and consistent volume will be suspended after 30 days and deleted from the program after 90 days.

2. Targeting mailbox providers
    - Your business cannot use a single IP address to send email to one specific mailbox provider.

Occasional and temporary single-receiver mailings may be tolerated under certain circumstances, but Return Path must approve it in writing.

3. Sending volume and IP limits
    - Certified customers are limited in the number of IPs that can be associated with their account. The table below reflects the maximum number of IPs allowed in Certification based on your contracted annual sending volume.

Sending Volume (Annually)	Maximum # of IPs
1,200,000	2
3,000,000	2
7,500,000	3
12,000,000	4
36,000,000	5
60,000,000	6
90,000,000	7
120,000,000	8
180,000,000	9
240,000,000	10
420,000,000	13
600,000,000	16
1,200,000,000	18
> 1,200,000,000	22

Part 3: 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 use 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
    - Your business is the only entity sending email over dedicated IP addresses for at least 60 days.
2. Open relays
    - Your infrastructure does not have any **open relay** servers.

3. FCrDNS
    - Your IP address reverse DNS (rDNS) entry matches the forward DNS entries, otherwise known as **Forward-Confirmed reverse DNS** (FCrDNS).
4. Blacklists
    - Your IP addresses or domains are not on a Return Path monitored blacklist. Return Path monitored blacklists. Repetitive or excessive blacklistings may result in the suspension or termination of your Certification benefits. **Learn more about blacklist thresholds below.**
5. SPF
    - All of your **Return-Path domains** have published **Sender Policy Framework (SPF)** records. **Learn how to set up SPF here.**
    - Your SPF records pass mailbox provider authentication checks within reasonable operational tolerance as determined by Return Path.
    - All **Return-Path domains** do not use a +all or ?all directive.
    - All **Return-Path domains** do not include a pointer (PTR) record.
6. DKIM
    - All of your email sent over Certified IPs have **DomainKeys Identified Mail (DKIM)** authentication configured. **Learn how to set up DKIM here.**
    - Your DKIM authentication passes mailbox provider authentication checks within reasonable operational tolerance as determined by Return Path.
7. DMARC
    - 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
    - You configure and maintain abuse@ and postmaster@ **role accounts** for all sending and **Return-Path domains** to handle complaints and other issues.
    - We also recommend you support and maintain other standard role accounts such as support@ or help@ accounts.
9. Domain Ownership
    - Your business must have full access and control over all sending domains, **Return-Path domains**, and website domains associated with the email sent from your IP addresses. To prove domain ownership and control over your domains, you may be required to update your DNS with a TXT record containing a unique character code provided by Return Path.

- This TXT record may be required to remain within your DNS record for the duration of your membership in the Certification program.

10. **List maintenance**
    - Your business uses email address list maintenance systems to reliably receive and process delivery errors, bounce messages, and other replies from receiving networks.
    - 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

We review your email message content to 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**
    - You send email that clearly uses your business's branding, such as a header or footer with your logo to accurately identify yourself to subscribers.
    - Text only mail must include a link to your website, your company or brand's standard signature, and your business's valid physical mailing address.
2. **Subject line**
    - All subject lines are accurate.
    - All subject lines clearly relate to the email body content without being deceptive or misleading.
    - 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**
    - All email body content is truthful and accurate.
    - For any commercial, promotional, or transactional mail, you must include your business's valid physical mailing address or your headquartered corporate address.
    - You do not use URL shorteners in your body content. This includes, but is not limited to, the use of Bitly or TinyURL.
    - You do not use a Report Spam link within your email body's content. This is typically used by senders who attempt to avoid mailbox provider complaints.
    - Attachments, regardless of file type, within any Certified mail is not permitted.

4. **Message headers**
    - The From and Friendly From name and address clearly identifies the Certified sender.
    - 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.
5. **Unsubscribe process**
    - Every commercial, promotional, or peer-initiated email sent over your IP address includes a **list-unsubscribe header** and an unsubscribe link.
    - Unsubscribe instructions are clear, conspicuous, and easily understood.
    - 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.
    - 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.
    - 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.
    - You process and fulfill all unsubscribe requests within 3 days of receiving the request.
    - 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.**
    - Unsubscribe links that are sent through any email remain active and functional for at least 60 days following the date it was sent.
    - 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.
    - 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 within 30 days that occurred between your business and the recipient.

Part 5: Disclosure

It's critical that you directly tell subscribers about the type of email they're signing up for, what they should expect, and more. This is done by reviewing how you collect email addresses, also known as your points of collection. Your disclosure must meet the following requirements:

1. Clear and simple
    - You have clear and simple disclosure at all points of collection where a subscriber enters and submits their email address. Including a link to your privacy policy instead of listing the information does not fulfill this requirement.
    - You must clearly disclose if you share or rent your subscribers' email addresses or any other related personal information at all points of collection.

Part 6: Consent

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:

    - **Confirmed (double) Opt-in:** After a subscriber opts into your email program, you must send 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.
    - **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 to opt out of promotional emails.

    - **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.

    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.

- At the point of collection, you clearly and conspicuously name the business from which the recipient is also signing up to receive email.
- You clearly define every brand from which a recipient may be signing up to receive email. Each brand has separate sign-up options, with no pre-selected checkboxes. This requirement also applies to brands that operate under the same parent company.
- 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

- The sign-up form includes CAPTCHA or reCAPTCHA to verify the legitimacy of the friend initiating the email. CAPTCHA and reCAPTCHA helps prevent bots or exploitative users.
- You only send one Forward to a Friend commercial or promotional email to the submitted address.
- If a Forward to a Friend email recipient does not respond, you can send only one follow-up email.
- The **Return-Path domains** are your own domains listed in the email header.
- The Friendly From name and address must clearly identify the Certified sender.
- You provide recipients with a way to unsubscribe from all future email, which is commonly referred to as a global unsubscribe.
- Emails do not contain links or URLs to external web addresses.
- Emails can include personalized comments up to 140 characters.
- An individual user can only use this feature to send a maximum of 100 messages over a 24-hour period.
- In order to send recipients of a Forward to a Friend email additional commercial or promotional email, they must opt into your email program by using 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

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
    - Your company must have a valid privacy policy that is easily accessible on your website's homepage.
2. Physical address
    - Your privacy policy includes a current physical address for your company. P.O. boxes are acceptable, although subscribers prefer street addresses. If your physical address is not present in your privacy policy, Return Path requires that it be found either on the home page or the contact us page of your website.
3. Point of Collection
    - 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.
4. Data Disclosure
    - 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. Brand Ownership
    - If you are a brand owned by a parent company, you must include the name of the parent company and your relationship with that entity in your privacy policy.

Part 8: Legality

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

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
    - Your email infrastructure is maintained and operated in a responsible manner.
2. Subscriber protection
    - 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
    - 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
    - You will notify Return Path in writing within 2 business days if you discover your IP or domain has been compromised.
    - 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 that 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
- Verizon Media Group (Yahoo!/AOL) Feedback loop
- Microsoft Junk Email Reporting Program

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
    - To resolve any Certification program-related issues, you and any team involved in sending email will cooperate with the Certification administrators.
    - 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
    - You maintain up-to-date contact information with Return Path.

Part 12: Performance and Compliance

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.

Exceeding any of these thresholds will result in suspension at the corresponding mailbox provider.

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: IPs that have 1 or more junk votes will be suspended if the Group SRD thresholds have been exceeded. Group SRD enforcement occurs when your total Certified IP count is greater than or equal to 2.

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

Complaint Compliance Thresholds (30-day average of all sending volumes)

Microsoft: Complaint Rate	0.2%
Yahoo!: Inbox Complaint Rate	0.6%
Comcast: Complaint Rate	0.3%
Yahoo!: Inbox Complaint Rate	1.0%

Tip: Having problems with your complaint rates? Check out this resource.

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

Spam Trap Compliance Thresholds (30-day cumulative)

Critical Spam Traps	3 Trap Hits
Significant Spam Traps	5 Trap Hits
RP Trap Network	100 Trap Hits
Cloudmark Traps	100 Trap Hits

Tip: Having problems with spam hits? Check out this resource.

Blacklist Compliance Thresholds (current listing)

Critical Blacklist	1 Blacklisting
Significant Blacklist	2 Blacklistings

Tip: Curious to know what blacklists we monitor? Check out this resource.

Need help?

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

Businesses run better and grow faster with trustworthy data. Tens of thousands of organizations rely on Validity solutions – including DemandTools, BriteVerify, Trust Assessments, Return Path and GridBuddy – to target, contact, engage, and retain customers effectively. Marketing, sales, and customer success teams worldwide trust Validity solutions to help them create smarter campaigns, generate leads, drive response, and increase revenue.

validity.com

sales@validity.com