SENDER CERTIFICATION REQUIREMENTS

validity

Contents

Introducing Certification

The Validity Sender Certification program provides access to exclusive data feeds and ongoing support from a team of Certification experts for the duration of your contract, in addition to the opportunity to become a Certified sender. Once you fulfill the necessary requirements to demonstrate your emails can be trusted and achieve Certified sender status, we will place your IP address(es) on our allowlist, and our mailbox provider partners will be notified of this change. Your placement on the allowlist will also start Validity's 24x7 monitoring of your IP address(es) to protect against security threats that could damage your sender reputation.

During any time your IP addresses are not Certified, you will still have access to the data feeds and our Certification experts will remain available to provide coaching on the changes needed to achieve Certification.

Customer Responsibilities

Sender Certification Questionnaire

Customers are required to complete the Sender Certification questionnaire ("Questionnaire") and are responsible for submitting the completed questionnaire to their Certification Analyst. The completed questionnaire enables your access to the data feeds and kicks off your email program audit for Certification. It is in your best interest to complete the Sender Certification questionnaire as soon as possible. Typically, customers are able to complete this within the first day.

The Validity Certification team will work quickly to review your responses, perform the audit of your email program, and compile a summary of any findings preventing you from becoming Certified. Any issues identified in this review are the responsibility of the customer to resolve in order to proceed with Certification.

Certification Maintenance

Customers are required to continuously fulfill the conditions set by the program to retain Certification status. The specified conditions will ensure you are aware of and adhering to industry standards and demonstrating your ability to be recognized as a trusted sender.

Become Certified

Sender Certification is designed to provide deliverability protection for reputable senders that follow industry-standard best practices and meet subscribers' as well as top mailbox providers' expectations. Throughout your process to become Certified, we will work together to ensure your program fulfills our program requirements.

By applying for Certification, you represent that your responses to the Certification program are complete

and accurate. Throughout the process, we may ask for additional information to confirm your email program meets Certification requirements. You must provide this information before you can become Certified, and promptly notify Validity of any changes.

Here are the key steps to becoming Certified:

1. When you subscribe to Sender Certification services, we will initiate a comprehensive audit of your email program, as requested, to ensure your program meets all the requirements detailed below.

2. You will be asked to provide our Certification Team with details about your email program. Once received, you will gain access to your deliverability data direct from our mailbox providers and filtering agency partners. This data will provide you with details on how your IP addresses have performed by allowing you to monitor complaint rates, spam trap hits, sending volume and more.

3. If your email program meets the requirements outlined in the Business Model, Measurability, and Infrastructure sections below, your account may be eligible for preliminary activation of the Certified status before the audit is complete.

4. If your program qualifies for preliminary activation, you will receive Certification benefits including access to Certification Program features and services for up to 60 days while we conduct our audit and you work on the required updates to become Certified.

5. 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. We recommend you complete any updates as soon as possible to ensure you are using the full services available within your subscription.

6. If your audit updates are not complete after the 60-day preliminary activation period or your IPs do not meet the requirements for Certification at any point during your subscription, your IP(s) will be suspended from the Certification allowlist. If suspended, you will still have access to your Certification data outlined above and we will continue to work with you and give guidance on corrections to be made to complete the audit and be re-activated to the Certification allowlist once all corrections are made.

7. Once all appropriate changes are made, the Certification team will finalize your audit and your Certified IP addresses will be added to the allowlist.

Certification Requirements Overview

To become and stay Certified, you will need to meet the requirements of the Certification program (“Certification Requirements”). 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 or regulations that impact you and your subscribers
- **Security:** show how you take care of your systems and subscribers' data
- **Communication:** communicate timely, clearly, and openly with Validity
- **Feedback loops (FBLs):** use complaint feedback to keep a clean, healthy list of subscribers
- **Performance and Compliance:** demonstrate your email program stays within performance 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 approved 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 IPs dedicated to your email traffic. Shared IP addresses with other entities 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, customer support emails, or 1:1 communications with business contacts and other third-parties.
- Certified IPs must send templated, clearly branded emails. They cannot send free-form content such as web forms or open text boxes.

IMPORTANT: We do not Certify businesses in any of the following categories:

Email Service 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 Members	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 Validity'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 offering one cent bidding to their customers.
Illegal Activities	Business operations or practices that may violate the law in a given jurisdiction.
Human Trafficking	Businesses operating for the purpose of illegally transporting people from one area to another.

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

- Each IP address sends at least 100 email messages to each Microsoft and Yahoo! over the most recent 30-day period, as seen in Validity's data sources.
- Each IP address maintains a 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. Validity must approve any exceptions in writing in advance.

3. IP Segmentation

- IP segmentation is the process of separating and sending email traffic from different IP addresses based on various factors related to your email program such as domains, region and mail type. The objective of IP segmentation is to organize your mail in such a way as to maximize performance to help ensure your email reaches the inbox. While not required, we highly recommend implementing an IP segmentation strategy for your email program. Learn more about IP segmentation here.

4. 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 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. SPF

- All of your Return-Path domains have 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 Validity.
- SPF Records do not use a +all or ?all directive.
- SPF Records do not use a pointer (PTR) mechanism.

5. DKIM

- All of your email sent over Certified IPs are DomainKeys Identified Mail (DKIM) signed. Learn how to set up DKIM here.
- Your DKIM authentication pass mailbox provider authentication checks within reasonable operational tolerance as determined by Validity.
- DKIM Keys have a minimum of 1024 bits. For additional security, we recommend 2048 bit key length.

6. DMARC

- You publish Domain-based Message, Authentication, Reporting & Conformance (DMARC) for each domain that sends mail from your Certified IPs. Learn how to set up a DMARC record here.
- DMARC must be set to at least p=none and in alignment with SPF and/or DKIM. However, all three policy flags (p=none, p=quarantine and p=reject) are acceptable within Certification.
- The authenticating domain must be the same domain found in the message From: header.
- The authenticating domain must have a "rua" value for processing aggregated reports from mailbox providers. It is recommended to monitor these reports either through Everest or through other DMARC reporting tools.

7. ARC

- If operating a forwarding service of any kind, we highly recommend implementing Authenticated Received Chain (ARC). ARC is an email protocol that helps preserve email authentication results and verifies the identity of email intermediaries that forward a message on to its final destination. Learn more about ARC here.

8. Role accounts

- You operate functional 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 verify 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 Validity.

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

10. List Hygiene

- 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 templated email content to ensure that your email follows best practices as expected by mailbox providers. This includes being transparent with your subscribers about who you are. Here are the email 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 commercial, promotional, or transactional mail, you must include your business's valid physical mailing address or your headquartered corporate address.
- URL shorteners are prohibited in your message content. This includes, but is not limited to, the use of Bitly or TinyURL.
- Links within the message body should be visible and easy to understand. Recipients should know what to expect when they click a link.
- 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.

- Don’t use HTML or CSS to hide content in your messages.
- Attachments, regardless of file type, within any Certified mail are not permitted.

4. Message headers

- The From address and Friendly From name clearly identifies the Certified sender.
- Email message headers are not falsified, obscured, deceptive, or misleading in any way. Message header Identifiers such as the Return-Path header, the From header, the Friendly From name and address must be accurate and operable.
- Message headers should be RFC Compliant including:
    - Every message includes a valid Message-ID.
    - No repeat use of single instance message headers in a message.
- Avoid excessively large message headers

5. Unsubscribe process

- Every commercial, promotional, or peer-initiated email sent over your IP address includes a list unsubscribe header (RFC2369) included in the DKIM signature.
    - The list unsubscribe header must meet RFC8058 as a one click unsubscribe function.
    - You must also have a message body link that allows a subscriber to remove their address from your mailing list. This link may direct subscribers to a preference page.
- Unsubscribe mechanisms are clear, conspicuous, easily understood, and user-friendly.
- The unsubscribe process does not require a recipient to provide any information.
- Once a recipient unsubscribes from your email program, you will no longer send them any commercial or promotional email, including a confirmation of removal. Additionally, you will not sell, lease, or share the unsubscribed recipient’s email address or personal information to any third party.
- You process and fulfill all unsubscribe requests within 2 days of receiving the request.
- You honor anyone’s request to unsubscribe from your email program indefinitely, regardless of subscription type, or until they opt into your program again. Learn about Certification’s opt in requirements here.
- Unsubscribe links remain active and functional for at least 60 days following the date it was included in your Certified messages.
- 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

You must 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.
- **Other Consent Methods:** If your email program relies on an alternative legal basis, other than consent for processing 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 critical to understand and comply with applicable laws and regulations that impact you, the standards of which may be higher 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 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 (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 one click 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.

4. 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 must adhere to any laws applicable to you in your operating jurisdictions. Your business should be fully transparent with potential subscribers about what data you collect, your email program, and how they can reach you. These 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, Validity requires that it be found either on the home page or the contact us page of your website.

3. Data Disclosure

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

4. 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 is the Customer's responsibility to understand, fully comply with, and follow these laws and regulations wherever you operate. Validity is not responsible for determining if a Customer's email program is legal. Customer's presence on the allowlist is not a determination that Customer's program is operating legally. A Customer's failure to comply with laws, however, will preclude them from participation in the Certification program. 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)
- State Specific Legislation

Canada:

- Canada's Anti-Spam Legislation (CASL)

Europe:

- General Data Protection Regulation (GDPR)
- ePrivacy Directive
- UK General Data Production Regulation (UKGDPR)

Australia:

- Spam Act of 2003

Brazil:

- Brazillian General Data Protection Law (LGPD)Part 9: Security

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, reliable, and security-conscious manner.

2. Subscriber protection

- Your business uses adequate, industry-standard policies and procedures to secure and protect your subscribers' email addresses and other personal data.

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 Validity in writing within 2 business days if you discover your IP or domain has been compromised.
- If your IP or domain is compromised, you agree that the IP or domain will not be re-enabled in the Certification program until Validity 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:

- Microsoft Junk Email Reporting Program
- Comcast IP and Domain Feedback Loop
- Yahoo! Feedback Loop

Part 11: Communication

Whether you are just beginning the Certification application process or you're already Certified, it's important that there is clear and open communication between your business and Validity. 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 initiate any required actions within 10 days of the notice.

2. Contact Information

- You maintain up-to-date contact information with Validity.

Part 12: Performance and Compliance

When you remain within the performance thresholds listed below, you receive reputation benefits at participating mailbox providers, improving your deliverability to reach more of your subscribers. Exceeding any thresholds will result in suspension in part or in whole.

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 (30-day cumulative)

SRD Volume	0-4	5-10	11 or More
SRD Rate	Not Enforced	5 Junk Votes	45%

Microsoft Group SRD Compliance Thresholds (30-day cumulative)

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!/AOL: Inbox Complaint Rate	0.2%
Comcast: Complaint Rate	0.3%
Cloudmark: 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.

Blocklist Compliance Thresholds (current listing)

Critical Blocklist	1 Blocklisting
Significant Blocklist	2 Blocklistings

NOTE: Repetitive or excessive blocklistings may result in the suspension or termination of your Certification benefits. Learn more about the blocklists that we monitor here.

Need help?

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

For over 20 years, tens of thousands of organizations throughout the world have relied on Validity solutions to target, contact, engage, and keep customers – using trustworthy data as a key advantage. The Validity flagship products – DemandTools, BriteVerify, Everest, GridBuddy Connect, and MailCharts – are all highly rated solutions for CRM data management, email address verification, inbox deliverability and avoiding the spam folder, and grid CRM applications. These solutions deliver smarter campaigns, more qualified leads, more productive sales, and ultimately faster growth.

For more information, visit Validity.com and connect with us on LinkedIn and X (formerly known as Twitter).

validity.com

sales@validity.com