MARIGOLD

Google & Yahoo! Sender Requirements:
FAQ

As part of the new sender requirements from Google & Yahoo, recipients must be able to unsubscribe with ease. Unsubscribe headers must comply with the one-click requirement. Be mindful that your existing unsubscribe link in the body of the message is still required and will continue to work.

We understand that these sender requirements are generating questions from your teams, so we have done our best to collect and answer these questions in this document.

If you have additional questions, please consider the following:

- Contact our Support teams
  - Campaign Monitor by Marigold Support
  - Emma by Marigold Support
  - Vuture by Marigold Support
  - Marigold Engage by Sailthru Support
  - Marigold Engage Support
  - Marigold Engage+ Support
- Work with your Marigold contacts to further explore your specific questions
- Watch the recording of our first webinar (simply register and access the on-demand recording)
- Refer to our Google & Yahoo Guide, by product, with additional recommendations and directions
- Read our recent blog posts

General Questions

1. **Question: Will these requirements be applicable in all regions? Will they apply to all organizations (i.e. universities, NPOs and non-profit organizations)?**

   Answer: The requirements for email authentication apply to anyone who sends one email or more to someone with a Google or Yahoo email address, regardless of the size or industry of the email sender. These requirements are also applicable globally, regardless of region.

2. **Question: If we use a Marigold product to primarily send to internal employees, do we still need to make changes for these new sender requirements?**

   Answer: If you send to any personal email addresses at gmail.com or yahoo.com, you will be required to make these changes. As they are best practices for all email, we recommend that you implement them for all services that you use to send email regardless of the recipients.

3. **Question: Can you please link to the blogs referenced in the webinar on Google postmaster and the content from Marigold?**

   Answer: You can reference our recent blog posts, including our 2024 Deliverability Guide and a recent blog post on the planned account deactivation from Google. You can read more about the Google Postmaster tools, made available by Google, from their blog posts.

4. **Question: Who should use and/or monitor Google postmaster tools?**

   Answer: We recommend sharing the insights and reporting from Google postmaster with the team or people responsible for ensuring your email campaigns are successfully delivered.

5. **Question: It appears that Google is recommending we send from a single IP address, or send from different IP addresses for various types of campaigns. How should we manage this if we need to send from multiple IP addresses?**

   Answer: There is no new requirement related to the number of IP addresses to send email. The best practice is to use separate IPs for marketing and transactional purposes, but the number of IP addresses needed is dependent on the volume of mail sent and may be more than one for each of those kinds of mail streams. That balance is managed by the Marigold Delivery and Infrastructure teams.

6. **Question: How should agencies or partners who manage / resell Marigold products manage these new sender requirements?**

   Answer: This depends on if the reseller and/or agency manages their customers' domains. If you do manage those domains, you can make the DNS record updates for your customers.

7. **Question: Who is the best point of contact if I have questions about the new sender requirements and implementing them?**

   Answer: If you have specific questions, we recommend you connect with your Marigold contact or a member of our Support team. See the top of the FAQ for links to our various product Support teams.

8. **Question: When do you recommend we make the required changes in order to be compliant?**

   Answer: If you do not yet have a registered domain (for example, you are sending from a Gmail or Yahoo email address), you should take action ASAP to purchase a domain. Domains must exist for at least 30 days prior to use, and this will be required as of February 1. If you already own a domain, you should still consider taking action sooner rather than later to ensure you are compliant and ready to go prior to the February 1 deadline.

9. **Question: If I have more technical questions, will there be a more technical workshop in the future to address these questions?**

   Answer: For customers using our Campaign Monitor by Marigold or Emma by Marigold products, we'll be hosting office hours in early January. For all products, we'll be releasing a detailed guide with product-specific instructions, as well as technical and roadmap webinars in January to review the product releases that support these new requirements.

10. **Question: Are there major differences between the requirements from Google and Yahoo? Do you expect other mailbox providers, such as Outlook, to also implement these requirements?**

    Answer: Google and Yahoo specifically coordinated to ensure that their requirements were the same for consistency and to avoid confusion for senders. We expect that other mailbox providers will follow with the same or similar requirements in the future. By implementing these changes for Google and Yahoo, you are implementing them for all mail that you send to all recipients. Unless other mailbox providers have different requirements, there should be no further action needed if they do adopt them. These are very broad and accepted best practices for all mail.

Domains

1. **Question: How do I purchase a domain if we don't currently have one for sending?**

   Answer: A domain can be purchased from a domain registrar, and there are hundreds of options available. We recommend looking at details like pricing, length of contract, and additional services (if needed) like website hosting or design. A few of the more popular options for domain registrars include Bluehost, HostGator, GoDaddy, and Domain.com.

2. **Question: How do I authenticate my domain?**

   Answer: Please refer to our product-specific guides for these step-by-step instructions.

3. **Question: How do I know if I own my domain? For example, you mentioned '@meetmarigold' is actually a gmail account.**

   Answer: Generally if you have an email address or website with some version of your business name, you or someone associated with your business owns that domain. Example domains that wouldn't be owned by you would be gmail.com, hotmail.com, yahoo.com, wix.com, facebook.com, and similar.

Authenticate your Emails

1. **Question: Are SPF, DKIM, and DMARC all required?**

   Answer: At this point in time, DKIM and DMARC are required, and SPF is strongly recommended. However, at Marigold, we recommend implementing all three records to avoid any additional deliverability issues in the future.

2. **Question: How do I set up SPF, DKIM, and DMARC?**

   Answer: Please refer to our product-specific guides for these step-by-step instructions.

3. **Question: What does it mean to authenticate my email?**

Answer: Authenticating your email means that you are sending mail that has SPF and a DKIM signature tied to the 'From' address shown to your recipients, and a DMARC record.

4. **Question: How can I verify that DKIM, SPF, and DMARC are successfully in place? Are there systems or sites that can verify?**

   Answer: We are working on tooling for some of our products to support this verification, planned for January 2024. However, in the meantime you can use third-party services for this verification. You can find additional recommendations HERE.

5. **Question: Do you recommend specific vendors for setting up DKIM, SPF, and DMARC?**

   Answer: You'll establish these DNS records, including DKIM, SPF, and DMARC in your respective domain registrar. Given there are hundreds of different domain registrars, we do not recommend any one specific vendor. If you already have your own domain name, those records will be managed where your domain is currently hosted.

6. **Question: How many engineering hours will these changes require? Do I need my IT team to participate in the updates?**

   Answer: Most of these new records can be set-up in less than a half hour. As long as you have access to your domain registrar, you do not necessarily need IT support to be successful.

7. **Question: How frequently do you recommend we update DKIM keys?**

   Answer: These recommendations are product-specific. Please contact our Support team for additional assistance or for added support.

8. **Question: Are there concerns if our subscribers are forwarding our emails to other Google or Yahoo email addresses?**

   Answer: The email systems that those are being forwarded from will also need to be compliant with the Google and Yahoo requirements. All mail from all sources must be compliant to be able to deliver messages to Gmail and Yahoo recipients. That forwarding will not impact your domain reputation in either case.

9. **Question: If multiple departments use a Marigold product, or we have franchises, or we have a parent / child account structure, do all accounts need to establish DKIM, SPF, and DMARC records? Is there an easy way to bulk make these updates for multiple accounts?**

   Answer: This may be slightly different based on each product. However, the requirements are structured for each domain, which may impact several more complex organizational structures with domains and subdomains. If you have specific questions, connect with your Support team for additional assistance.

10. **Question: If we send emails from a different name (for example, on behalf of my boss), will this be a problem?**

    Answer: As long as you're sending from the same domain, for example my email is megan@meetmarigold.com but I am sending on behalf of my boss with john@meetmarigold.com, you will be okay as it relates to these requirements. However, keep in mind that using a different name or an unknown email address may cause your subscribers to mark the unknown email as spam or not open your email.

11. **Question: If we want to add additional actions for DMARC, such as quarantine, how can we set-up the protocols to ensure that happens?**

    Answer: Moving to a quarantine or reject policy should only be done after a thorough identification of all sources of email from your domain to ensure that they are all DMARC compliant. All in-house, third-party tools, third-party applications, any system sending email from your domain must be authenticating those messages with either SPF or DKIM. DMARC allows for reporting about those mail sources and their compliance but you will generally need to utilize a third-party service to consume those frequent and potentially high volume reports. Those services provide reports and analysis of compliant and non-compliant systems for you to follow up on. Enabling a quarantine or reject policy will disrupt email delivery from non-compliant sources.

12. **Question: Can you explain ARC requirements and how they might be different from DMARC records?**

    Answer: ARC is most relevant to systems where email forwarding is in use, including membership in a Google Group or other kind of list where many people can communicate with many other people. Emails that pass through that system must have an ARC signature added by the group or list software that directs whether a message from someone posting to the list passed Authentication when it was received. Once it is forwarded on to the other members of the group, that authentication status cannot be determined without that ARC signature.

13. **Question: Do you recommend publishing reverse DNS records for the public?**

    Answer: Reverse DNS must be public for all IP addresses that originate email.

14. **Question: What are MTA-SNS DNS records and do you recommend them?**

    Answer: MTA-STS is a mechanism by which domain owners can require that email sent using those domains must be encrypted while in transit. MTA-STS is still in an early adoption stage and there are still significant gaps in support by both senders and receivers. We do not recommend implementing it at this time.

15. **Question: What will happen to unauthenticated emails? Will they be marked as spam or simply not delivered?**

    Answer: Either action is possible. Gmail and Yahoo are expected to make decisions about which action to take based on their internal data. Spam rate will be an important measure and as you approach 0.3%, your messages are more likely to be rejected at the time of delivery.

Make Unsubscribing Easier

1. **Question: What is the difference between opt-out and unsubscribe?**

   Answer: They are functionally the same; the recipient no longer receives messages from that sender (optionally related to a specific topic that they had originally subscribed to if supported by the unsubscribe system). The new distinction is that these mailbox providers want two different mechanisms to accomplish that. The first is the same as it has always been -- a clearly visible unsubscribe link in the body of the message. That link can go to a landing or preference page to confirm their desire to change their mailing preferences or unsubscribe entirely. The new requirement is a defined URL in the headers of the message that they can submit on behalf of the recipient that will unsubscribe them from the related mail stream without further action by the recipient. This will allow mailbox providers to display a clearly visible and consistent unsubscribe option within their own interfaces to their users.

2. **Question: Is double opt-in (i.e. email and click) a best practice or a requirement?**

   Answer: It is currently a best practice in the context of the new requirements. Both Gmail and Yahoo have indicated that future requirements will be based on current best practices.

3. **Question: If the new standards require an unsubscribe link to be in the header of an email, do we still need an unsubscribe option in the body of an email as well? Footer?**

   Answer: Yes. Unsubscribe options must be included in the header (new requirement) as well as the footer (existing requirement). The difference between the two is that the unsubscribe option in the header must be one-click, while the unsubscribe option in the footer can lead to a preference center. You must still provide the footer unsubscribe option for all recipients to be compliant with the various anti-spam legislation.

4. **Question: If we send our unsubscribers to a separate landing page for preferences, will we still be able to do this under the new requirements?**

   Answer: You will still be able to send unsubscribers to a preference center but only via the unsubscribe option in the footer. The unsubscribe option in the header must be one-click, so there's no option to route to a preference center from there.

5. **Question: Will the unsubscribe link in the header mean the contact is opting out of all emails we send or just emails using that particular audience list?**

   Answer: This may vary by product and audience set-up. Please work with our Support teams for specific guidance.

6. **Question: What's the difference between one-click and two-click unsubscribe? Is there a preferred option?**

   Answer: In the context of these new requirements, one-click unsubscribe is based on a header that Gmail and Yahoo will ready to present an unsubscribe link within their applications. For that one, the subscriber must be able to click that link and be unsubscribed without any further action. In fact, Gmail and Yahoo will submit that on behalf of the recipient so no further action would be possible. Two-click unsubscribe can be thought of as taking the recipient to a landing page where they may be asked to confirm their desire to unsubscribe, or perhaps choose to modify their subscription preferences instead.

7. **Question: How can we ensure that the unsubscribe request is processed within two days?**

   Answer: The various Marigold products will automatically handle the unsubscribe within our applications within that time window. If you have a third-party data source that also needs this information, you will need to ensure that it is also updated within that time frame.

8. **Question: In the past, we have had up to 10 days to manage unsubscribes? Will this new 2-day requirement override that 10-day requirement?**

   Answer: Depending on where you are located, you may have seen local or national regulations in place regarding time to respond to unsubscribe requests. While those regulations may still exist, it is likely that the new two-day requirement from Google and Yahoo is a faster response time. Be sure to stay compliant with the two-day requirement if sending emails to users with Google or Yahoo email addresses. Non-compliance can impact your ability to deliver messages to those recipients.

9. **Question: How does the unsubscribe link relate to requests via emails from our audience asked to be removed from future email campaigns?**

   Answer: There is no connection. You should continue to handle those requests as you receive them.

10. **Question: How do I make sure that my customers only unsubscribe from promotional emails and not transactional emails as well?**

    Answer: This is likely a function of your unsubscribe options in tooling like a preference center or audience lists, and may be product-specific. Please work with our Support team for additional guidance.

11. **Question: If we have removed the opt-out option in an email, per our Compliance team, will the new unsubscribe link make this null?**

    Answer: Generally, any messages to gmail.com or yahoo.com addresses must have the one-click unsubscribe header present. However, there may be some product-specific exceptions for suppressing this requirement for specific senders. Please work with our Support team.

12. **Question: If we have a custom email template and have removed the unsubscribe link, will the new requirements force us to now include an unsubscribe link in the header? Can this be avoided?**

    Answer: Generally, any messages to gmail.com or yahoo.com addresses must have the one-click unsubscribe header present. However, there may be some product-specific exceptions for suppressing this requirement for specific senders. Please work with our Support team.

13. **Question: Are there simple ways to identify dormant or inactive subscribers and remove them in bulk?**

    Answer: There are some options for identifying segments of users, based on the specific Marigold product(s) that you are using. For the complete answer and additional information, please contact our Support teams.

14. **Question: How can we make it easier for those who have unsubscribed to re-subscribe?**

    Answer: This is both a tactical question, as well as a strategic question. For members of your audience to re-subscribe, you need to strategically make it appealing to do so. This might mean more targeted or personalized content, increased automation like journeys, or even new subject lines to capture the attention of your audience. However, before you can improve your strategy, you need tooling to allow your audience to re-subscribe. This is product-specific, so please work with our Support teams for additional guidance and best practices.

15. **Question: If we add unsubscribers back into our lists, especially if they unsubscribed accidentally, will we be penalized?**

    Answer: Adding people who unsubscribed back to a list is risky and not strongly discouraged. In cases where a subscriber has explicitly indicated their desire to be re-added to the list and is not able to do so themselves, that is generally ok. Where a subscriber has unsubscribed and you do not have that explicit knowledge and permission that they want to resubscribe, then doing so goes against their explicitly stated preference to not receive email. Continuing to email them is likely to generate complaints and impact your mailing reputation, and may lead to blocking or other more significant implications.

16. **Question: We offer an opt-down option to reduce the cadence of emails - how will this work / will it work alongside the new unsubscribe requirements?**

    Answer: This is product-specific. Please work with our Support teams for additional guidance.

Steer Clear of the Spam Threshold

1. **Question: How do I know what our current spam rate is?**

   Answer: You can sign up for Google Postmaster Tools at https://postmaster.google.com. You'll be asked to prove ownership of your domain, then they will provide you with various metrics about your email to Gmail recipients, including spam-rate. Note: Postmaster tools provide metrics only if you send sufficient mail to Gmail recipients.

2. **Question: How do I manage hard and soft bounces more effectively?**

   Answer: Hard and Soft bounces are managed by the Marigold platforms based on industry standards and expectations. You should generally not alter those statuses unless you have clear knowledge that they are somehow incorrect.

3. **Question: Is the spam complaint rate of 0.3% based on a single day or over a period of time?**

   Answer: At this point in time, we don't have a clear answer from the teams at Google and Yahoo about the measure of time for measuring spam rates.

However, it is fair to assume that a single day of higher-than ideal spam reporting will not impact your overall spam rate.

4. **Question: How frequently are spam complaints reviewed?**

   Answer: At this point in time, we don't have a clear answer from the teams at Google and Yahoo about the frequency of reviewing spam complaints. However, as we learn more from these teams, we'll continue to share that information with you.

5. **Question: What are the consequences of going over the spam threshold?**

   Answer: Both Google and Yahoo have indicated that both spam folder placement or full delivery rejection are possible actions based on their internal metrics. As you approach the 0.3% spam rate threshold it is more likely that your messages will be blocked, but is only one of several metrics the platforms use to make that determination.

6. **Question: If we're seeing an increase in hard bounces, what does that mean?**

   Answer: Broadly speaking, it generally means that the mailboxes you are attempting to send to are no longer valid. Gmail has recently begun work to delete all accounts that have not been accessed in the past 2 years, and will continue to do so going forward. That may play a part in hard bounce increases.

7. **Question: We're already having trouble with emails landing in spam folders and we have an opt-out list. What else can we do to avoid this?**

   Answer: The first step in resolving spam folder placement is understanding what signal or measure is leading to poor inbox placement. This can be caused by a variety of factors, most often this is associated with complaints but can also be a result of poor list hygiene, or a large inactive file. The leading cause needs to be diagnosed before a strategy can be implemented. Our teams at Marigold can support you in best practices for ensuring emails are delivered to the intended mailbox more often.

8. **Question: Is the spam rate calculated by the individual user or by ESP? For example, would we be penalized if the overall Marigold spam rate rose above 0.3%?**

   Answer: The spam rate is calculated by individual accounts, rather than for the whole of a product or a whole ESP. Therefore, your spam rate is only influenced by your specific lists, audience, and campaigns. Marigold is here to help you build better campaigns and use precautionary best practices to avoid being unnecessarily reported as spam.

9. **Question: What is sender reputation and how do we find it?**

   Answer: Sender reputation is a broad term that represents your trustworthiness, reliability, and general adherence to expected email industry standards and best practices. How it is measured varies by each mailbox provider based on the information available to them but is centered around how recipients are treating the messages that you are sending to them. Each provider will have their own reputation determination for you. Positive reputation comes from recipients actively interacting with your messages – reading them, responding to them, saving them, tagging them, moving them out of spam if they landed there, etc. Negative reputation comes from recipients ignoring your messages, deleting without reading them, marking them as spam, and other similar behaviors. There are also higher level things that providers look at such as whether you are authenticating your messages, honoring opt-outs, if your domain is on any block lists, etc. Gmail is one of the very few, if only, mailbox providers that gives you insight into your sender reputation before they start to action messages sent from you negatively. This can be found as the Domain Reputation value in Google Postmaster Tools. As Gmail is usually one of the top recipient domains for senders, it's generally a good, but not exact, proxy for your overall sender reputation at most providers.