

Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Best Practices for Sending Legally Mandated Emails to Large Audiences

Version 1.0 Originally Published December 2020
Version 2.0 September 2026

The reference URL for this document is: <https://www.m3aawg.org/legallymandatedemails>

Audience

This document is primarily intended for email service providers (ESPs) who assist brands in sending mandated communications to large audiences.

Introduction

There are many scenarios in which senders may be legally mandated to send a bulk message to email addresses that have previously opted out, been suppressed, or have not been mailed to in more than a year. These messages are not intended to be used for standard marketing or transactional notices; they are exceptions to the rule. Prominent examples of mandated emails include breach notifications, product recalls, health and safety notices, or court-mandated communications, depending on the applicable jurisdiction.

High-risk messages are intended to inform individuals of a significant policy change and typically include information to help account holders mitigate damage suffered, offer assistance, or provide noncommercial information related to their account, such as instructions to reset a password or an offer of free credit monitoring. It is important to distinguish between high-risk communications, such as terms and conditions updates, versus legally mandated messages, such as class action notifications. This document addresses the latter. Senders may want to consider applying similar actions and requirements for sending high-risk communications, including terms and conditions updates, as these messages meet comparable legal criteria.

While each organization should determine if these mailings are worth the risk as compared to other forms of communications, such as adding the mandated message to an existing email, care should be taken to ensure messages are not overly intrusive. This M³AAWG Best Practices document is intended to help senders comply with legal requirements mandating that email be part of the communication strategy in a court order; however, it should not be taken as legal advice.

Tasks for Responsible Parties

Three broad roles — the brand owner, infrastructure operator, and deliverability consultant — are responsible

for different, sometimes overlapping, responsibilities when sending emails. The following outlines each responsible party's tasks:

The **infrastructure operator**, typically an IT staff member, is responsible for configuring the mail server infrastructure. If an Email Sending Platform (ESP) is used, the infrastructure operator is also responsible for configuring email sending through the ESP in accordance with the ESP's recommended customer best practices. The ESP has a shared responsibility to configure the infrastructure. Some aspects may be controlled by IT staff, who also have crossover responsibilities with the brand owner and deliverability consultant. The ESP is rarely the brand owner and may provide deliverability consulting services for customers, but not always. For this use case, these operators should consider establishing a preferred breach or mandated email process in their contract or Data Protection Agreement.

The **deliverability consultant** helps the brand owner understand how to comply with email sending best practices and assists the infrastructure operator in delivering email. In many cases, the infrastructure operator also makes deliverability decisions. The ESP does not typically make those decisions unless it also offers deliverability consulting services to brand owners.

The **brand owner** is the business or organization legally required to send the notifications. Typically, the brand owner is also the entity that has access to modify the Domain Name System (DNS) for the domain(s) used to send email. Additionally, the brand owner is able to determine when alternative communication channels should be used instead of email, when necessary.

Brand owners cannot defer the following responsibilities to other parties unless the other parties are explicitly under contract for that purpose:

Technical Considerations

- To preserve its domain reputation, the brand should use a clearly identifiable subdomain for mandated notifications so that the receiver clearly recognizes the notification is associated with the brand, for example, notice@sub.brand.com. When possible, the brand should avoid using a new domain, cousin domain, or a variation on the normal sender domain when emailing notifications.
- The sending organization should be unequivocally verified with domain authentication. Emails should be sent from a domain owned by the brand responsible for complying with the mandated email requirement.
 - Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC) must be configured for the sending domain.
 - Please refer to the [M³AAWG Email Authentication Recommended Best Practices](https://www.m3aawg.org/sites/default/files/doc_files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf)¹ document for detailed recommendations.
- IP addresses used for the sending infrastructure must have proper Forward-Confirmed Reverse DNS (FCrDNS) in place. Each IP address must have DNS with a PTR record that resolves to a hostname, which in turn resolves back to the IP address.
 - Alternatively, for an ESP, it may be simpler to have a small, dedicated subnet of IP addresses for mandated email, regardless of the brand or sender involved. This allows mailbox

¹M³AAWG, Email Authentication Recommended Best Practices, September 2020. Available at: https://www.m3aawg.org/sites/default/files/doc_files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf

- providers (MBPs) to configure those IPs with DNS that best suits this type of email sending.
- Some mailbox providers encourage reserving an IP range exclusively for mandated email notifications. If a dedicated IP or subdomain cannot be obtained, senders should plan for a cooldown period after the campaign. After a large-scale, legally mandated send, the IPs or IP range used for the campaign should not be used for unrelated sending streams until their reputation has recovered.

Message Audience

- The brand owner should determine the appropriate recipients based on the specific requirements of the court order or mandate. A phased sending strategy should prioritize recipient groups from highest risk to lowest risk, beginning with those who are most engaged. This helps ensure that critical notifications are sent to the highest-priority recipients before any delivery issues could affect subsequent sends. The suggested order is as follows:
 - Impacted users
 - Active users
 - Subscribed users
 - Unsubscribed users
 - Bounced users (although due to recipient error, this may not be received, but it may still be legally required depending on the mandate).

Message Structure

- Use an appropriate *From* name, for example “[Organization or Product name]: Notification.” While this is not a typical recommendation, this identification can help clarify the relationship between the notification address and the brand.
- Use a clear and concise subject line that states that the notification is important and distinctly different from other communications.
- Use an appropriate template style that is plain or minimal in appearance for the notification type.
- Send emails with minimal use of tracked elements in the message. For example, brands should limit links to those that are required, or none at all. The message should contain only material exclusively relevant to the issue, with no marketing or other content.
- Message accessibility may be mandated as part of the communications. Frequently, court-mandated messages carry their own specific accessibility requirements, such as plain language obligations, screen reader compatibility, and translation for non-English speakers. Following these requirements is necessary.

Suggestions for Brand Owner

Brand owners should coordinate the following activities to ensure mandated emails are delivered effectively and in accordance with applicable legal, operational, and technical requirements:

- Provide the order of required activities, as well as any legal guidance, such as instructions and timelines from relevant regulators or the brand’s legal teams.
- Consider suspending marketing communications during the notification period. By avoiding high throughput and volume peaks, which may be onerous to receiving networks and trigger anti-spam mechanisms, and batching sends into smaller segments, messages are more likely to be successfully received.
- Coordinate a consistent message across all customer service teams. This includes social, call center, and

frontline staff interacting with customers.

- Determine if a mandated email requires proof of send for auditing purposes, which is often the case, and what that proof entails.
- Inform the infrastructure operator or their ESP of the email.
 - Some ESPs will not allow customers to send this type of email due to the risk it imposes on the ESP's reputation and its deliverability of other mail streams.
 - ESPs may provide technical requirements, best practices, consulting services, or features to help maximize the message's effectiveness and minimize its impact on the sending IP address and domain reputation.
 - The ESP may require the brand owner to procure dedicated IP addresses, so that any deliverability issues, including IP rate limiting or message rejections, are isolated from other customers using the ESP's shared IP address pools.
 - When working with clients to send notifications, ESPs may have limited ability to influence message content, as the content will often be written by legal counsel to ensure the organization fulfills its responsibilities under the notice.

Alternative contact methods

Using email for notifications is sometimes unavoidable, but in some cases other forms of contact can be used depending upon the court order. Drawing the brand's attention to other options may be advantageous to both parties, particularly when email may not be the most effective method of notification. This can occur when the addresses on file are inaccurate or abandoned, automatic filtering mechanisms identify emails as bulk mail and divert messages away from the inbox, or users overlook or disregard unexpected emails, regardless of the subject header field. Brand owners and their ESPs may wish to raise alternative notification methods with courts or regulators during the early planning stages, unless the mandate specifically requires email.

There are several other ways to reach recipients, including, but not limited to, the following:

- Website notification
 - Ideally, this should be a publicly accessible domain-aligned web page which includes information about the mandated send, including the date, notification, affected parties, and other details. This may be prudent even if the website does not have logged-in users who can receive push notifications via HTTP.
- Push messages in the organization's app
- Notification delivered by the postal service
- Social media posts
- Traditional media channels, including newspaper, radio and television
- Mobile messaging platforms, including SMS, MMS, RCS, OTT and other common messaging services in the region where the recipients reside.

Postmaster Reachout

If the deliverability consultant determines a preemptive postmaster reach-out is necessary, the following details should be provided approximately 1-3 weeks in advance to allow recipients to prepare:

- Appropriate contact details for the organization or agency where recipients can get more information, as well as a copy of the message itself, if possible, or a link to this information.

- The expected sending volumes, rather than the total cross-MBP send volume, broken down per receiving mailbox provider and days required. This may be provided by the brand or determined in another manner, such as the list of users that meet the court-mandated criteria.
- The appropriate sending infrastructure, including the sending domains and hostnames that will be used.
- Dates and times, or a range of dates and times, if sending over an extended period.

Conclusion

When considering the target audience for these notifications, some recipients are inherently more challenging to reach, making alternative methods of communication worth considering. For known bounce addresses or users who have previously reported a brand as spam, ESPs may wish to consider alternative contact options such as postal notices or notifications in relevant newspapers. It is important to remember that although this type of sending carries reputational risks, the notifications are likely of special relevance to the recipient. This special circumstance justifies mandated emails in the rare instance of a compulsory notification as defined in the introduction.

Appendix

Examples of Relevant Regulatory Resources

- GDPR Articles 33–34 (personal data breach notification)
- HIPAA Breach Notification Rule (45 CFR §§ 164.400–414)
- CCPA and CPRA notification requirements
- U.S. state breach-notification statutes (e.g., NY SHIELD, CA Civ. Code § 1798.82)
- CAN-SPAM (where it intersects with required disclosures)
- Court-ordered class action notice (FRCP Rule 23)

As with all documents that we publish, please check the M³AAWG website (www.m3aawg.org) for updates.