



## **Allowlisting Information**

To ensure ePledge emails don't get rejected by SPAM filters:

The Email Communication Service sending/originating IP Addresses listed below should be added to spam filter allowlists and set as exempt to rate controls. Not allowlisting the sending/originating IP Addresses or not exempting them from rate controls can lead to rejected emails or slow delivery.

- smtp1.upicsolutions.net (52.86.171.35)
- smtp2.upicsolutions.net (34.232.26.125)
- smtp3.upicsolutions.net (34.230.104.208)
- mta-70-25-157.sparkpostmail.com (156.70.25.157)
- mta-70-25-156.sparkpostmail.com (156.70.25.156)

If the Email Communication Service IP Addresses cannot be allowlisted and exempted from rate controls, several features have been implemented to help reduce the misclassification of email communications from United Way.

These features are industry best practices to ensure email deliverability and reduce spam emails. To find out more about these features, please use the URL links provided below.

### **SPF Record (Sender Policy Framework)**

- This record defines what IP addresses can send emails on the behalf of a domain
- <http://www.openspf.org/Introduction>

### **DKIM Signing (Domain Keys Identified Mail)**

- When an email is sent through the Campaign email service, it is automatically signed with a special signature.
- The receiving party verifies this signature by looking it up a special DNS record.
- <http://www.dkim.org/#introduction>

### **DMARC (Domain-based Message Authentication, Reporting & Conformance)**

- DMARC builds on top of SPF and DKIM and helps define what should happen when a message fails checks through SPF and DKIM as well as where to send failure reports.
- <https://dmarc.org/>