# Email Communication Service

Please review the information below regarding the Email Communication Service. The Email Communications Service affects campaign-related emails, newsletters, and other forms of email communications used to keep you informed about our work and upcoming events.

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

Email Communication Service sending/originating IP Addresses:

- smtp1.upicsolutions.net (52.86.171.35)
- smtp2.upicsolutions.net (34.232.26.125)
- smtp3.upicsolutions.net (34.230.104.208)

If the Email Communication Service IP Addresses cannot be whitelisted and exempted from rate controls, several features have been implemented to help reduce the misclassification of email communications from United Way. The first feature is the use of SPF records and the second is DKIM signing of all emails from our Email Communication Service. The final enhancement, DMARC, will be implemented in late 2018. 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 (DomainKeys 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/