

A White Paper

## **VerticalResponse, Email Delivery and You** A Handy Guide

**VerticalResponse, Inc.**  
501 2nd Street, Suite 700  
San Francisco, CA 94107

Tel. 415.905.6880  
Fax. 415.808.2480

[www.verticalresponse.com](http://www.verticalresponse.com)

# VerticalResponse, Email Delivery and You

## A Handy Guide

Delivering email seems pretty straightforward, right? You upload a mailing list, create an email, hit send, and then mighty wizards transport that email to your recipients through the use of ancient, handcrafted cables and powerful laser beams. What more could you possibly need to know about this process? As it turns out, loads more.

There are a number of factors that determine whether an email, especially a bulk email, gets a response from its recipients. What are those factors? I'm glad you asked!

Let's start by looking at the journey an email goes on to reach its intended recipient. In order for an email to be properly delivered, it must pass through one or more "gates", each of which has the power to deny that email passage and stop it from continuing on its way.

## The Email "Gates"

### Gate #1 – The Internet Service Provider (Yahoo, AOL, Comcast, etc.)

Getting through this gate is all about the reputation of your sending IP Address. This reputation is determined through a number of factors:

#### 1. Do you get complaints?

Complaints come in through a variety of sources: the Report Spam button at an ISP, through a blacklist, or directly to the abuse desk of your own service provider (like VerticalResponse). A complaint rate as low as 1%, or sometimes even lower, can have an impact on your delivery.

#### 2. Do you hit spam trap addresses?

Spam traps are addresses that are never used to sign-up for email or have been deactivated by the host ISP after a long period of inactivity. These addresses are often placed on web sites in order to tempt spammers to harvest them (nothing a spammer likes more than a big, juicy email just innocently sitting around on a webpage, waiting to be plucked), which makes it easier to find and stop mail sent by said spammers. A purchased or rented mailing list may contain traps.

#### 3. How high are your unknown user rates?

Having a lot of unknown users on your list (read: a lot of bad addresses) is a sign to a recipient ISP that you have poor mailing practices. Does this mean there's a problem if you see a high bounce rate following a single email campaign? Not at all. But if you regularly see bounce rates approaching 10% or higher, then something isn't quite right and you're more likely to encounter problems seeing your good addresses delivered.

# VerticalResponse, Email Delivery and You

## A Handy Guide

### Gate #2 – The Corporate Domain

“Corporate domain” refers to a domain belonging to an organization like VerticalResponse, SalesForce, or any other business that uses an internal System Administrator or process to handle their computer and email issues. Obviously, an email going to a Yahoo or Hotmail address wouldn’t have to deal with this gate, but there are hundreds of thousands of smaller domains that do fall under this category.

Many Sys Admins employ blacklists in order to keep spam out of their networks, so one of the best ways to ensure delivery to a corporate domain is to stay off of commonly used blacklists. Now, what’s a blacklist exactly?

A **blacklist** is a database of IP Addresses (and sometimes domains) that have been used, or may have been used, to send spam. These lists are used by recipient servers to stop mail from the listed IP Addresses (or sometimes domains) from getting through.

There are literally hundreds of publicly available blacklists at a Sys Admin’s disposal. Some of them are large, effective and very popular (like Spamhaus and SpamCop) and some of them are small, use questionable methods to create listings, and are hardly used by anyone (I’ll avoid referencing any of those so as not to hurt their feelings). Each blacklist provider has their own methodology for determining which IP Addresses should be listed and which listed IP Addresses can be removed if requested.

In addition to these publicly available blacklists, some companies use their own private, internal blacklists that are only put to use for their domain or domains. These are not public, so the only way to know you’re listed is to send mail to the recipient domain in question and see if you receive a bounce error saying you’re listed. If you are listed, you have to try and track down their Sys Admins and request removal.

Staying off blacklists is mostly all about one thing, and that one thing is not getting complaints. The best way to not get complaints is to only mail people who’ve specifically requested information from or about your company. As luck would have it, this is exactly what VerticalResponse requires of our clients.

# VerticalResponse, Email Delivery and You

## A Handy Guide

### Gate #3 – The Spam Filter

Even if your IP Address has a good reputation and you haven't been receiving complaints, there is still one final gate through which your email must pass: the spam filter. Email Service Providers like Yahoo have their own filters and individual corporations usually use an outside filter (like Postini or SpamAssassin). Each filter is different in its own way, but there are still some general issues to consider to help you avoid seeing mail filtered to the spam folder:

#### 1. Reputation

Spam filters provided by Internet Service Providers consider reputation not only when allowing your email through the main gate, but also when determining whether your email should be filtered or go into the inbox. Your reputation may be good enough to reach this point, but bad enough to get you filtered if your content is really spammy looking. In reverse, a good reputation can also help you overcome some spammy content (but it all depends on the situation and the content involved).

#### 2. Content

This one is obvious and is all about making sure your email doesn't look like spam. At one point, not looking like spam mostly just meant not using "gotcha" words and phrases like "Free Loan Just for You and Family!" or "Open This Right Now!" or "\$5000 dollars, free inside for you my best friend!" Now it can also mean not sending image only / image heavy emails (as 50% of spam is image only at this point) and making sure your HTML code is properly formatted and clean.

# VerticalResponse, Email Delivery and You

## A Handy Guide

### **What Does VerticalResponse Do to Ensure Excellent Delivery?**

#### **We're Anti-Spam**

Everyone says they're anti-spam, but we really, really mean it. We respond to and investigate every single complaint that comes in to our abuse desk, we quickly deal with clients who receive complaints (before they start causing delivery problems), and we even look over every email our clients launch to make sure nothing suspicious or fraudulent can make it out the door. This keeps complaints to a minimum, which is a big part of maintaining a strong reputation for our IP Addresses.

#### **We Automate Bounce / Unsubscribe Processing**

By automating this process (like many of our competitors), we ensure no users can abuse our IP Addresses by ignoring bounces and unsubscribes. This also helps us keep an excellent reputation.

#### **We Use Feedback Loops**

We have feedback loops set-up with every single ISP that is known to offer one. This means if someone clicks Report Spam at Hotmail, that Hotmail trusts us to take action on the complaint. It also means that when someone clicks such a button at a participating an ISP (like Hotmail), VerticalResponse users don't have to worry they'll accidentally send mail to that person again as we automatically unsubscribe recipients who treat a client's email in this way from that client's list.

#### **We Use Authentication Protocols**

We authenticate client email through the use of the three currently major authentication protocols: SPF (Sender Policy Framework), Sender-ID and DomainKeys. With SPF and Sender-ID we have published records that state our mail domains are allowed to send email on behalf of our own IP Addresses. With DomainKeys we sign each email with a key that the recipient server can then use to verify that we actually sent the email. These are a very important part of maintaining a good sending infrastructure.

# VerticalResponse, Email Delivery and You

## A Handy Guide

### **What Can You Do to Help Ensure Excellent Delivery and Response?**

#### **Keep a Clean Mailing List**

Be sure everyone on the mailing list has specifically requested info from or about your company. Also make sure you're not mailing previously unsubscribed or bounced addresses. That went out of style a long time ago.

#### **Treat Subscribers with Respect**

Don't mail subscribers too often and clutter their inbox with mail they don't want. Set expectations at the time of sign-up: "This is what we're going to send you. And we're going to send it to you this often." Also try to maintain a relationship with the subscriber. Don't mail them sporadically once or twice a year and expect them to take action with your emails.

How often is too often? How sporadic is too sporadic? I would say once a week to once a month is a good range to keep in mind.

#### **Design With Delivery in Mind**

Don't just put a big image together in Illustrator and think you're good to go. Make sure the email is easy to read (consider paragraph length and fonts), that images are being used only to enhance the HTML / text content (not as the sole content), and that the email is something that the subscriber would expect to receive based upon their sign-up.