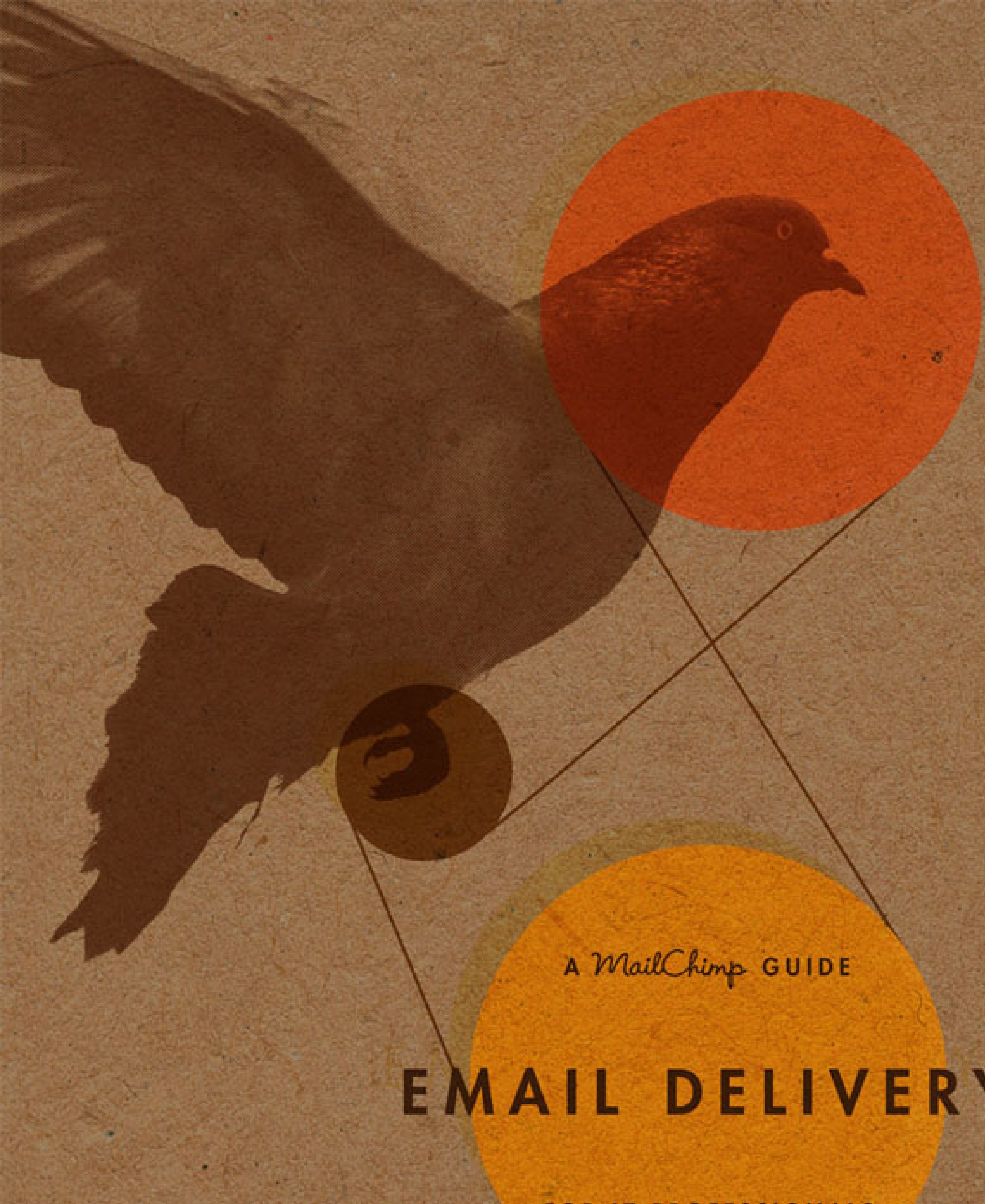

A MailChimp GUIDE

EMAIL DELIVERY

FOR IT PROFESSIONALS

MailChimp

email delivery for IT professionals

INTRODUCTION

So you've been asked to put together an *email marketing blaster cannon thingamajig*. Maybe your CEO is trying to save some bucks. Maybe the marketing team is trying to get better tracking (to ask the CEO for more money). Or maybe you're a big nerd and like setting up servers. Whatever the case, you're the poor schmuck that has to figure out how to get the email marketing blaster built. My name is Brandon Fouts, and I'm the deliverability engineer at MailChimp. We send a few hundred million emails a month, and I'm here to help you understand how to set up your deliverability infrastructure (or you could just sign up free for MailChimp, and we'll send out your email for you). Either way, if you're an IT person in charge of deliverability for email marketing, then you've come to the right place.

There's lots of buzz about the changes that companies sending commercial email will face with ISPs. In the old days, ISPs tracked abuse complaints and bounces and a few other basic stats to determine the reputation of an IP or sender. In the new world order, companies will not only be faced with preventing abuse complaints and bounces, but they'll also have to start worrying about engagement. Each ISP will have its own engagement algorithm to determine how readers are responding to mail. Tracking engagement is more complex than monitoring a few stats. ISPs will be concerned with subscribers opening, clicking, unsubscribing, marking as spam, deleting, etc., so the person managing the list has to be even more conscientious. The marketer better be sure that what he's sending is engaging, or his email will go straight to the spam folder—or, worse, get blocked.

But it's easy for companies to miss an important aspect of deliverability. You've got to have a great deliverability infrastructure to compete. For example, if you're delivering engaging content to a 100% double opted-in list but your MTA isn't configured correctly, or you're not set up to process abuse complaints, you're headed for trouble.

In this guide, I've included real-world scenarios and vital information for understanding the complexities and hurdles involved with setting up your delivery infrastructure and keeping that infrastructure running. MailChimp wants to help you understand the role infrastructure and management play in deliverability, and how to leverage your infrastructure in a way that will help your marketing team deliver engaging content. Most of the information in this guide is targeted at the technical and social requirements for setting up your delivery infrastructure. If all this stuff is in place you have a far better chance of hitting the inbox.

Before getting in too deep, you might want to check out our terminology section. Let's get started.

HOSTING AND HARDWARE

Choosing the proper hosting facility is a big part of designing your delivery infrastructure. Whether you're going into an existing data center or looking for a new one, you should keep a few things in mind.

First, you should NOT use cloud environments like Amazon or RackSpace Cloud, as these environments are in no way suited for sending email. They're also home to spammers, so it’s best to keep your sending IPs off these networks. Make sure you're with a reputable hosting facility for your sending network.

And you don’t want your MTAs to live in the cloud or in a virtual environment. MTAs need bare metal and fast drives. An MTA’s activity is bound mostly to disk and CPU, so cloud and virtual environments aren't suited well to the task. Consider this when you're thinking about your network topology and designing your application. Your sending infrastructure (or at least your MTA) may have to exist in another datacenter. We've seen the effects of tying your sending infrastructure in the cloud, and the results are poor performance and reputation.

Some delivery applications are built so that the agent builds the email up at the agent level and hands it off to the MTA, while other agents are designed to package the needed data and let the MTA handle the email's construction. Both have pros and cons, but when your application is in the cloud and the MTA may have to live elsewhere, it’s important to pick the agent option that limits your bandwidth. If you're mostly in the cloud or in a virtual environment, ensure that your application is developed in such a way that the MTA does not have to exist in the same network/environment as the application.

IP/DNS

So you have the email addresses necessary to start, but no domain to attach them to—or maybe you *do* have a domain to attach them to, but don't know where to go from there. If you're sending commercial email for your domain, it's best to attach your commercial email to your domain in some capacity. If you're sending email out for some other company or have no idea where to start with IPs and domains, then this section will help.

DNS Naming

You likely fall into one of several categories:

I already have a domain.

Let's say you have the *example.com* domain and you want to send a bunch of marketing email to your list of opted-in email addresses. The first thing to understand is the effect that sending commercial email can have on your domain.

If you're not sending to a legit list, then you're putting your domain at risk. Just engaging in commercial sending is risky, so you better plan carefully. If you prefer to keep your domain out of the mix because there's too much at risk, then you can use a different domain. Just remember that everyone associates you with *example.com*.

The next step to consider is using some form of a sub-domain. For instance, *mail1.example.com* is a possible sub-domain. Choose your domain, sub-domain and naming conventions wisely, as this can have a significant effect on your deliverability and how ISPs and anti-spam authorities view you. As always, think about growth here, and use some letter and number scheme for your sub-domain—do NOT use a numbering scheme for your root domain. It's best to associate ONE domain to one client if you're using a dedicated IP scheme.

I'm sending on behalf of someone else.

Let's say you're sending for someone who's not tied to your domain. Do NOT, under any circumstances, tie your client's commercial email to your domain. For example: Say you're a design agency, and Joe's Bait & Tackle wants you to send email for them. We'd advise you to use and associate all email traffic to Joe's Bait and Tackle's domain. *Using your own domain for this will affect your domain reputation.* Try to tie their commercial email to their domain or create a new domain. The same rules as above apply when it comes to naming conventions. (Choose your domain, sub-domain and naming conventions wisely, as they can have a significant effect on your deliverability and how you're viewed by ISPs and anti-spam authorities. As always, think about growth here, and use some letter and number scheme for your sub-domain.

I'm sending on behalf of several companies.

Let’s say you're sending for several companies at once. The first determination you need to make is whether to use a shared or dedicated IP scheme. Later, we’ll describe the differences and reasons you'd use one versus the other. Again, same rules apply: Choose your domain, sub-domain and naming conventions wisely, as this can have a significant effect on your deliverability and how you're looked upon by ISPs and anti-spam authorities. As always, think about growth here, and use some letter and number scheme for your sub-domain—do NOT use a numbering scheme for your root domain (*mail.example1.com*). If you're using a pool of IPs for several customers, ensure that the domain is consistent for that pool of IPs. In other words, don't use different domain names in the shared IP pool, but use the *xxxx1.yourdomain.com* schema.

IP Ranges

It's important to think about how much email you're going to be sending, and depending on your sending volume, you can determine how many IPs create the right balance.

Generally speaking, you don't want too few IPs, in case you experience more volume than you expect. And you don't want so many IPs that you look suspicious or spread out your volume over too many IPs. There has to be a balance of volume to IP/domain.

ISPs know who you are, and they know your IP blocks. They're probably smarter than you are, and if you think your little ol’ operation isn't being watched, you're sorely mistaken. They see all and know all, so get this aspect right.

Sending too much volume from an IP, sending from too many IPs or sending too little from a range of IPs can all lead to deliverability issues. So what's the right number? Word to the Wise had a couple of posts about this in a series of articles (Article 1, Article 2, Article 3, Article 4) that will give you some insight into the right balance for you.

Test IPs

Before you send over your IPs, visit Sender Score and Sender Base (and AOL) to find out the history and reputation of your IP. You don't want to get an IP block with a bad reputation from your registrar or hosting company.

Registrars

It's important to use a reputable registrar. Use one that has high standards and, most importantly, takes abuse seriously. Don't associate your IPs with a registrar known to be used by spammers. If you're going to register domains or purchase IPs through a hosting facility, read through our Hosting and Hardware section for some pointers on choosing a good hosting facility.

From Address

The *from* address you use should be associated with the same domain as the from domain in a dedicated IP setup, and the same domain where the signup occurred.

WHOIS Contact Information

When you register your domains, apply ALL of your information to the WHOIS information. Make sure the physical address information is listed, along with the organization name that's associated with the email. Also ensure that the contact email addresses for abuse and other info is present in the WHOIS record. *Do this for all domains and IP addresses, and check each and every record if someone else sets this up for you*. The WHOIS information is important when registering for whitelisting, FBL and other registration processes. If the WHOIS records don't match up with the company making say, a Microsoft SNDS request, you'll be unable to register. With Microsoft SNDS you have to ensure that your WHOIS records match up to with the rDNS of the IPs you're registering. Something to avoid is domains by proxy and any other privacy service to mask IP/domain ownership, etc. This is frowned upon by most postmaster desks.

Reverse DNS

Setup forward-confirmed reverse DNS for your IP/Domains. Do this before you register anything with ISPs, providers or do any type of whitelisting.

MX Records

Ensure your MX Records are properly configured. Generally, your hosting facility will help with the setup of this. Check the records at MXToolbox or DNS Stuff.

Shared IPs

If you're sending out for multiple clients or customers, sometimes it’s better to use a shared pool of IP addresses. The volume or frequency from one client or department may not warrant a dedicated IP. We'll discuss throttling in more detail a little later, but ISPs throttle your sending volume. If you send too much, too fast, they'll bulk you or reject the email. Conversely, if you send too little or infrequently, ISPs can respond the same way.

Using a shared IP pool, you can put several clients into the pool, and this will keep sending frequency consistent. When you're using a shared IP pool, you want to get your number of IPs right so that you're sending the right amount over each one.

The downside to a shared IP pool is that a sender or set of senders can affect the reputation of the others. Throughout this guide, we'll share some techniques to help with this scenario, but its important to know that your IP or domain is what ISPs are generally looking at to determine reputation. Most people would say, “Then that's a good enough reason to put everyone on a dedicated IP!” But again, sending too little or infrequently can be as damaging as sending too much.

One more note on a shared IP: Make sure your development team or your code that hands the email off to the MTA is properly and evenly spreading your email over the pool of IPs. In other words, don't let IP1 get 80% of the content and IP2 get 20%. If you see that you're sending too much volume and deliverability drops, add another IP or set of IPs. Ensure that your pool of IPs is segmented by domain. If you need several pools, use the domain to denote the pool and the sub-domain to differentiate each MTA/VMTA.

Dedicated IPs

If you plan to send lots of volume (50-75K twice a week), send frequently (10-15K daily) or send transactional messages, you'll want to use a dedicated IP for that traffic. In some cases you may need to use a pool of IPs for the dedicated traffic. In that case make sure that the IPs carry the same domain with different sub-domains. Dedicated IPs are great because the traffic is isolated to that specific client/department. But it’s important that if you choose to use dedicated IPs that your sending is consistent and the quality is high. It's your traffic and ONLY your traffic, so nobody else is at fault if things go bad. Dedicated IPs should be whitelisted. See the Word to the Wise ISP Information to find all the whitelists.

Transactional Messaging

We advise you not to send transactional messages (signups, unsubscribes, online receipts, etc.) over the same IPs or domains as marketing-related email. Instead, separate and segment these message types into their own "worlds." If you include these messages in the same domain/IPs, you won't be able to apply for whitelisting on those domains/IPs.

Also, if someone wants to unsubscribe from your weekly newsletter but still receive their online bill, you'd want that traffic to go over different domains so that if they block the newsletter traffic or unsubscribe, they still receive their bill.

Publish Your IPs

Make sure you publish your IPs somewhere on your site. Use them for reference and to allow people to whitelist (or blacklist) you.

MTA

We highly recommend using a commercial MTA product to effectively manage multiple IPs/domains, error correction/handling and to have the best connection/sending to ISPs. We use PowerMTA from Port25, and its an incredible product and serves out lots of email. Why should you use a commercial product? Because things will break (or you'll break something), and you'll need someone smart enough to fix the disaster when things don't come back up like they should. Other benefits of using a commercial product are that they understand what you want to do with their product, and they'll help you with configurations and maintenance.

MTAs

There are lots of commercial and free MTAs available. Some popular MTAs include Power MTA, Message Systems, Cold Spark, postfix, qmail, and strongmail, but there are many others. Commercial products generally provide benefits over the open-source products, like monitoring and configuration user interfaces, configuration for administrators and general ease of use.

So you've got all these domains, IPs, servers, etc. Now you have to match this IP to that MTA, set up to send really slowly to Yahoo and faster at certain times to this other ISP, and then there's that Russian domain you have to send really slowly to…

This is the tough part, getting the all configurations dialed in.

There are several levels of configuration, and it's important that all these settings are properly tuned. You have configurations at the server level, domain level, virtual MTA level and domain-specific to the ISP. We recommend starting with the default configurations to see what works best, and then tweak as you go along. You'll find that what works for another sender may not apply to your infrastructure. This is one of the reasons we recommended you buy a commercial package—so you can get proper support during this process.

The other important factor with configuration of the MTA is that when all is said and done, you need to test, test and test some more.

Security

As with all your infrastructure, security is extremely important. Your delivery infrastructure is precious and vital. It's the type of system that can be used maliciously in the wrong hands, and there's plenty of precious email data to steal. Don't do anything silly like allowing open relay. Secure your infrastructure behind a firewall, and better yet, require VPN access to get to your systems. That includes the monitoring and dashboard utilities. Secure anything and everything that is related to your delivery infrastructure.

Rate Limiting

Another critical step in the MTA configuration is rate limiting or throttling. Rate limiting allows ISPs proper time to process and filter spam and ensure that transactional email doesn't get backed up. Without rate limiting in place, ISPs would be even more overwhelmed than they already are. The ISPs all have different sending limits on a per hour, per day basis. ISPs can throttle your sending volume when it’s too high or too low. If you send too little volume, they won't really know who you are and bulk your email. Consult with your MTA vendor for proper configuration for rate limiting. And don’t think you can just get away with simply sending as fast as possible—you'll fast-track yourself to getting completely bulked or blocked.

Error Correction/Handling

Once you hit thresholds with the rate limits, send too much spam, or have any number of other issues, the ISP may start returning error messages. A good commercial MTA will allow you to handle these errors and adjust.

Some ISPs will want you to slow down the sending, stop sending for a period of time, or change your habits (due to bad engagement, bad reputation, etc). Most commercial MTAs have recommended settings and then allow further customization for when errors occur. Take this aspect of your setup seriously, because failure to do this will get you in some serious trouble. Understand that each ISP is different. Also, some of this stuff changes throughout the year, and ISPs develop new error codes that will require you to tweak settings and configurations to respond to the changes. You'll need resources to attend to tweaking the configurations and keeping an eye on error correction to ensure it is working properly.

Authentication

If you're going to send email in any commercial capacity (even if you don't send commercially), you have to use some form of authentication. We highly recommend using all four forms, and if they (whoever "they" is) come out with a new one, then use it, too. Do NOT listen to someone who says authentication is optional. Some ISPs can bulk your email if you don't send with their supported/recommended authentication method. Some ISPs use authentication as a factor in determining whether an email is valid. If you don't have authentication in place, you might make it to the inbox, but if the content is questionable or the history of the IP/domain is poor, then you could see higher levels of bulking.

We have a cool chart and details about authentication here.

The four primary forms of authentication you want to set up are:

SPF

Setting up Sender Policy Framework is easy to set up, and it makes it harder for spammers to spoof an email from your domain. You can even cheat with the SPF setup wizard.

Domain Keys

Domain Keys are still used by some smaller ISPs, but DKIM is preferred by most. If you want to ensure delivery, you can sign with Domain Keys but it’s not an absolute requirement.

DKIM

It’s important that you fully understand DKIM and have it configured properly. Note that the d= portion of your DKIM signature can be configured to point to a different domain. For instance, if your MTAs domain is mydomain.com, you can configure your DKIM signature to use another domain or your client’s domain. This is becoming an industry standard and highly recommended so that the from domain and DKIM signature match when sending traffic over a dedicated IP.

SenderID

Authentication developed by Microsoft and used by several big ISPs.

Testing Authentication

After you get all your authentication set up, you need to test it.

Start by testing with the port25 verifier, which is sends an email to check-auth@verifier.port25.com. After that works successfully, you need to do real testing with the major ISPs.

Send an email to the ISPs that use the various authentication types and make sure the email passes properly. Even if it gets to the inbox, you should physically open the email, look at the headers, and make sure it’s passing authentication. After you go through all the details of setting up your delivery infrastructure, the last thing you want is an authentication error causing your email to be blocked.

BOUNCE HANDLING

Bounce handling is a critical factor in your delivery infrastructure. When you send to a bad email address or an email account that is full the receivers server will return a message with the bounce reason. The bounce message will contain a Diagnostic-Code header that will give the bounce code, reason and any other information that may be pertinent to the bounce. Not only do you need to be able to "clean" bounces, but also you may have to handle soft bounces differently from hard bounces (and in some cases you need to handle the bounce as though it didn't bounce). Unless you want to manually clean bounces, you have to have a bounce processor in your application that takes in bounces and processes them accordingly. This can get complicated, because bounce reasons aren't fixed and can be customized by the receiver. So a 521 with Joe's mail server might be a hard bounce, but a 521 with Jane's mail server might mean something totally different. Below we'll try to describe ways to make this easier:

VERP

Your sending applications, API or whatever is handling the construction of the email to pass to the MTA needs to include a variable envenlope return path (VERP) in the header. A VERP'd address looks something like this:

some_unique_identiefier(s)-therecipient=theirdomain.com@mail1.yourdomain.net

Notice that you put the recipient’s email address in that string. You do this so when the bounce occurs, you can get the email address out of the bounce record and handle the bounce accordingly. Your unique identifier(s) might be a unique customer id or account id, etc. Your application has to be able to parse the VERP'd address and record the bounce accordingly, so include what's necessary to record the bounce.

Hard Bounce

A hard bounce is an email message that is returned to the sender because the recipient's address is no longer valid. A hard bounce could occur because the domain doesn't exist or because the recipient is unknown. Here's an example of a hard bounce diagnostic code:

Diagnostic-Code: smtp;550 5.1.1 - Invalid mailbox: xxxxxx

Generally, you should process hard bounces as soon as possible, but you may want to build a policy that allows two consecutive hard bounces before the address is removed. You don’t want to keep sending email to a bounced email address, as ISPs include this as part of their formulas. If you're sending to a bunch of bad addresses, it could mean you have an old list, which ISPs and ESPs factor in when determining whether or not your list is bad.

Soft Bounce

A soft bounce is an email message that is returned to the sender because the mailbox is full or for other reasons. Here is an example soft bounce diagnostic code:

Diagnostic-Code: smtp; 552 xxxxxxxx MAILBOX FULL

Generally, you want to process soft bounces after a certain number of occurrences or a certain number of sequential occurrences. So if an address soft bounces X times in a row, you should remove them from your list. We recommend making that "X" number configurable, and you can determine whether to use consecutive bounces or bounces over the life of the email. Just remember, a soft bounce can be a temporary issue, and it’s possible the address is valid.

Bounce Categories

Something that can get frustrating is that bounce categories can be anything the receiver’s mail administrator wants them to be. Administrators can throw out specific bounce categories for your IPs/domains, bounce all your messages because you're blacklisted, OR they could use bounces for reporting bulked email. In other words, you should be able to distinguish bounces and even worry about some administrators mixing soft and hard bounces.

Categorization

Now we know that bounce categories are all over the place, and a soft bounce could be a hard bounce from a certain domain, or maybe you were blacklisted and a bunch of email bounced. What do you do?

Categorize bounces based on codes or diagnostic information. In other words, set up a way to store regular expressions and if a match is found, you re-categorize that bounce. If you know Joe's email administrator throws a 521 with the message "your IP XX.XX.XXX.XXX is listed on uribl" when you're on a blacklist, you can record that as a soft bounce or as spam-related, so that when the block is removed you will be able to send to Joe again. You need to build something into your bounce processing code that will take a bounce, look at the diagnostics provided, and categorize it appropriately if there's a matching regular expression and new category.

FBL (FEEDBACK LOOPS)

Feedback loops allow you as a sender to get reports from most of the major ISPs when someone reports your email as spam. Essentially, you register with the ISP to become part of the FBL process, and when someone clicks "Report Spam," the ISP will send you a specially formatted request in ARF format.

The email that's returned should be processed as soon as possible, and the recipient should be unsubscribed or removed from the list. This is yet another process that you would need in place unless you wanted to deal with these manually.

Also, it's important to mention that email headers play a big role in FBL processing. Information is vital, as not every ISP supplies a standard ARF report including VERP addresses and even custom headers denoting account, email, etc. They don't have to include the recipient in the returned email, and they can and will munge your headers. In most cases you can bank on having your headers intact, but that’s not always guaranteed. Make sure your FBL process has the capability to look at multiple headers and, if it fails to process that, it alerts someone to handle it manually.

Keep in mind that the subscriber’s email address can be fully redacted from the headers, so you may need to embed an email ID or an encrypted email address you can easily look up. An example could be something as simple as a header X-FBL:

campaignID.listID.emailID.

FBL is important because if you fail to remove a person who reported the email as spam, it can lead to serious problems. If you continue sending to the person who complained, they can very easily report you to blacklists, ISPs, your registrar and/or your hosting facility. All of those will affect your deliverability and reputation.

You should also keep a history of the abuse complaints. It's fine to keep the FBLs in an email account, but it's extremely helpful to store the data so that it can easily be retrieved and statistics can be gathered. You need to have this information available at your fingertips.

FBL Registration Resource

Word to the Wise has a great resource for ISPs that allow you to participate in their FBL program. It's critical that you register all of your

IPs. If you have a lot of IPs, this can take a while, so be sure to leave yourself enough time to work through each registration process.

Before you start registering, make sure you use the correct email addresses for all the setup. Don't use your personal email address for anything—use the role-based emails that you set up earlier.

Some ISPs will require you to setup FBL via an account with their domain (e.g. Yahoo). Yahoo requires that you use DKIM in order to get their FBL data. Most ISPs are using Return Path for FBL processing, which has a great FBL process. Microsoft's JMR program is their FBL program. It does take some time and requires that your IP registrar confirm that you're the owner of the IP ranges you're registering. Leave yourself plenty of time to get this set up before starting to send.

Some corporations and larger technology companies will send ARF reports. If you're going to be sending large amounts to a specific domain, contact the abuse department or email administrator at the domain to see if they offer FBL reporting.

FBL Maintenance

As you add IPs or domains, you'll want to register your new IPs/domains for FBL and all other whitelists, abuse.net , etc. Register the new IPs/domains prior to sending any email from them. It's also a good idea to check once or twice a year that everything is still in place with the ISPs.

Email Headers

If you're going to do commercial email in any capacity, you need to have control over your headers and provide some industry standard information.

Below are the most commonly found headers in commercial email. You can use your MTA to help with some of these and with using merge features to munge data into your headers.

Reporting Abuse

You didn't setup that *abuse@* address for nothing! You can do two things to allow people to report abuse.

The nicest way is to include a link they can copy/click in the header, which will take them to a page that provides some details of who you are and a form to fill out about the incident. That report is sent to your *abuse@* address to process. The other method is to include a message like "*To report abuse send an email to: abuse@abusexyz.com*". Either way you choose, you need to use an *X-Report-Abuse* header.

List-Unsubscribe

Some of the major ISPs will turn on images and show a special little icon if you include a List-Unsubscribe header that includes an unsubscribe link. This should be a link to an unsubscribe form, as some of the major ISPs are now integrating with this header to use this link instead of reporting spam. The presence of this header can turn on images with some senders, put a special icon in the inbox/email to denote a safe sender, etc.

Here is a great resource that discusses how to implement the List-Unsubscribe header.

Unique Identifiers

You should include some unique identifiers in your headers. These would be things that you could identify if someone were to send a header with redacted information.

Depending on how your system is engineered, you may need to include an Account ID, Campaign ID and Subscriber ID. You could combine this into one header, such as an X-Data header in the format of X-Data: *company_name.account_id.campaign_id.subscriber_id*

It’s important that, for security purposes, you obfuscate each of those values. You don't want to be using unencrypted data of any sort.

GETTING STARTED WITH SENDING

Warm-up

It's important to have a process in place for warming up IPs. First, check your IP’s reputation with Sender Score and Sender Base (and AOL). If everything's OK with your IP reputation, you still can’t just send a bunch of email out from a fresh new IP. You need to warm up the IP and start building a reputation for the IP and domain. Send 100 the first day, 200 the next, and so on. Slowly work up the volume and spread it out over a 24-hour period.

Some MTAs have the warm-up capability built in and will gradually increase volume and handle all this for you. Keep in mind that the ISP is getting to know you and learn your content and traffic patterns, so the warm-up phase is critical. It’s good to give it a few days and allow the ISP time to learn who you are. If problems arise, give it some time before contacting the ISP.

Hotmail generally requires slow sending from an IP, and if you don't slowly warm up the IP, you'll have issues that require you to visit their postmaster site to contact support to clear it up. Again, don't just contact them from the first use of the IP—if you do everything right, you won't have to contact them. If your IP reputation isn't so good, then you'll want to warm up much more slowly, and you may have to work with each ISP in repairing the reputation. Any time you contact an ISP, ensure that you've reviewed the ISP's requirements, fully investigated the issue and fixed any issues you're aware of that need to be addressed.

Whitelisting IPs/Domains

When dealing with dedicated IPs/domains, you need to go through any and all major whitelist registrations. You can register shared IPs/domains, but some ISPs will allow this and others won't (and don't try to lie—they know what you're up to). Also note that some whitelists have terms of service/use that allow the listing company/group to boot you for certain behavior. In other words, once you're on, that doesn’t mean you'll remain on. If you get in bad standing, you may have to re-register or perform certain steps to get back in good standing.

Whitelisting Registration Resource

Word to the Wise saves us again with a great resource on whitelists.

These are tedious, so leave yourself plenty of time. Generally, you'll need to get some sending under your belt before you can register. Usually 15 days is enough, but sometimes you can get away with less. Take the time to register with all the whitelists and, just like FBL registrations, make sure you maintain these. If you're denied whitelisting, try again in 30 days ONLY if your sending quality improves.

Abuse.net

Register with abuse.net so people can get in touch with you about unwanted email. It’s like a big lookup database for abuse contact information tied to IP/domain.

DNSLW

Register with DNSLW, which is commonly used by SpamAssassin.

Certification

A few companies provide IP certification. This isn't one of those things you can pay for and you're in the clear to send what you want. The companies who do paid whitelisting have a vetting process to bring you on as a customer, and they'll want to analyze your sending history, content, etc. before bringing you on. It's generally worth it if you can spend the money, but each one has its own caveats.

SenderScore Certified

Return Path provides Certified sender certification , which is essentially high-end whitelisting and covers a large ISP footprint. It'll improve deliverability and help almost immediately once it kicks in. It also turns on images automatically and has other various useful features with ISPs. The downside to SenderScore certification is that you're required to maintain a high level of deliverability. You have to stay within their boundaries, and if you go outside those boundaries, you can temporarily or permanently lose the certification, depending on the issue. If you attempt to send shared traffic over a SenderScore certified IP, you'll permanently lose your certification.

Safe Sender Certified

This is the same as the SenderScore certification, but for shared IPs. The footprint of ISPs it covers isn't as far-reaching, but it's better than nothing. It essentially gives you a negative spam assassin score to begin with, so if your content is good quality you should see good delivery. Similar rules to the SenderScore certification apply, so you need to maintain a certain level of quality with this certification. If you begin sending too little traffic or have high abuse complaints or bounces, you can lose your certification.

Goodmail

Goodmail certification is similar to SenderScore certification, but instead of the traffic going out of your IP, it's going out over a certified Goodmail IP. In other words, Goodmail replaces you and sends for you. When using Goodmail with many senders, you'll get a special badge that shows up in the email client to show you're a safe sender, and images and video are automatically turned on. This provides a high level of deliverability, but the downside is that if you have to stop using Goodmail, your IP/domain will have NO reputation. Because you send through *their* IPs, your IP isn't getting any traffic. Coming off of Goodmail would require planning so that you could properly warm up your IPs.

DELIVERABILITY TOOLS

It’s important to have good visibility into your deliverability. Below are a couple of products and tools that can help.

Return Path

Return Path offers several different products and some great tools to give you insight into how good your delivery is (or isn’t). They offer tools for previewing campaigns in over 30 email clients with spam filtering analysis, reputation monitoring, seed list monitoring and blacklist monitoring. The most valuable tools are the seed list and campaign monitoring, which allow you to import a seed list into your list and send to most of the major ISPs. It then collects the delivery stats as to whether the message ended up in the inbox, bulk or missing. The reputation monitor Return Path provides is somewhat helpful to use as a data point in determining if an IP has issues, but it should just be a data point, as not all major ISPs are providing data. Definitely a great set of tools and great customer service.

Unica

Unica recently purchased Pivotal Veracity. This is another delivery monitoring tool with a good reputation. We can’t speak directly to this tool, but we do know that a few ESPs use it heavily and are generally happy.

Microsoft SNDS

Microsoft offers the SDNS tool and should be used as a secondary tool to troubleshoot issues and gather information. The tool allows you to register your IPs and shows you information such as number of spam traps hit, abuse complaint ratio, and volume per IP. A great tool to check when a client is having delivery issues to hotmail/msn/live.

MONITORING AND EXCEPTION REPORTING

Once you're sending, you must have monitoring and reporting in place to understand the health of your infrastructure.

Engagement Monitoring

You need to continuously monitor the behavior of your IPs. One critical monitor you should have in place is the use of seed lists. You can have your application randomly add them into campaigns or include them in lists to measure your inbox placement. If you have one dedicated IP or domain you're sending from, just place a seed list into your list(s). If you have several IPs and domains in use, then randomly place the seed lists and watch your inbox placement in some automated fashion. Remember not to use the seed lists too much, as they can start having a negative effect on your list performance because those emails are not opened or responded to.

Also set up monitoring and analysis tools for determining how many emails are bouncing, how many people are opening or clicking in the email, how many unsubscribes are occurring, and how much FBL activity is occurring per IP and/or domain. It's vital that you track this information, because ISPs and email administrators are keeping a close eye on this. If you see high abuse complaints, unsubscribes or bounces, then you know something is wrong with your list-collection techniques. If you're experiencing low opens and clicks, it could be due to poor inbox placement, poor use of content or lack of proper segmentation.

Scraping MTA Logs

Set up some form of monitoring on your MTA logs. Most MTAs will have ways of handling exceptions, but they won't be able to handle all exceptions. For instance, some ISPs will report back if your IP is on a blacklist. That's something you want to be aware of in real time. You should set up some scripts to actively monitor your IPs and domains to check the major and minor blacklists. But you also want to actively mine this data in your MTA logs. Some ISPs and Blacklists don't have a way to look up your IP’s status, so by scanning logs you can catch the exceptions that might occur. There are other scenarios where you want to scrape MTA logs for spam trap addresses, fatal errors, etc. Make sure you can easily search your MTA logs to troubleshoot issues.

Static/Dynamic Error Handling

We touched briefly on using your MTA to handle certain errors that might occur and mentioned scraping your MTA logs to find out when errors occur—but note that there are different types of errors that require different types of actions.

The first type is a static error. This is the type of error Comcast might throw when you're blacklisted. They'll throw a diagnostic code that looks something like this:

Comcast block for spam. Please see
http://help.comcast.net/content/faq/BL000000

Now, if you weren't scraping your logs for this error or using your MTA's error handling, you'd never know this error took place. This is why we recommend using both the MTA error handling AND the log scraping as a means to alert you to issues. In this instance, you would have your MTA back off sending and allow enough time for you to resolve the issue. You may even switch all traffic to another MTA, etc. Your MTA should be able to handle all of this.

The next step would be to find out what's causing the issue. Having the scraped and searchable logs is key here. Find out the what, who and where of the incident. Fix the issue, and if it’s a specific email, list or customer, then stop the sending if necessary. Then, you have to manually fill out the Comcast unblock form and AFTER you receive the unblock notification, you can properly turn the traffic back on. Failure to fix the issue or error will cause all email to bounce going forward.

There are other errors we'll call dynamic errors. Some ISPs, like Yahoo, will throw a dynamic error that requires you to slow down or completely stop your sending for a few hours and retry when they throw a specific error. Similar things occur with almost all ISPs, and it’s important to configure your MTA and your log scraping to alert you so that your infrastructure can properly respond. If dynamic errors continue for an IP/domain, you need to investigate the cause and remediate. That might involve speaking with the ISP to find out the cause, but do your investigative work prior to going to the ISP. There are tons of codes and resolutions, and the ISPs add new ones each year. To summarize, this aspect is important, and you should work with your MTA vendor and your development team to build an application and infrastructure that's fully aware of these errors and can handle them cleanly.

Blacklist Monitoring

As stated in a previous section, there are several monitors and tools that can help you find out if you're blacklisted. Those monitors are great, but they don't get *all* of the blacklists, and most monitors will not be "real time" enough for your needs.

Here's a list of the major and minor blacklists:

AHBL, ANT, Backscatter.org, BARRACUDA, BURNT-TECH, CASA-CBL, CASA-CBL+, CASA-CDL, CBL, CYBERLOGIC, DEADBEEF, DNSBLINFO, DULRU, EMAILBASURA, FABELSOURCES, FIVETEN, GIRL, GRIP, HIL, HIL, HILLI, ICMFORBIDDEN, IMP-SPAM, IMP-WORM, INTERSIL, ivmSIP, ivmSIP/24, KEMPTBL, KUNDENSERVER, LASHBACK, LNSGBLOCK, LNSGBULK, LNSGDUL, LNSGMULTI, LNSGOR, LNSGSRC, MSRBL-Combined, MSRBL-Images, MSRBL-Phising, MSRBL-Spam, MSRBL-Viruses, NERD, NETHERRELAYS, NETHERUNSURE, NIXSPAM, NJABL, NJABLDUL, NJABLFORMMAIL, NJABLMULTI, NJABLPROXIES, NJABLSOURCES, NLKUNBLACKLIST, NLKUNWHITELIST, NOFALSEPOSITIVE, NOMOREFUNN, ORID, OSPAM, PDL, PSBL, RANGERSBL, RATS-Dyna, RATS-NoPtr, RATS-Spam, REDHAWK, RRBL, SCHULTE, SDERB, SENDERBASE, SERVICESNET, SOLID, SORBS-BLOCK, SORBS-DUHL, SORBS-HTTP, SORBS-MISC, SORBS-SMTP, SORBS-SOCKS, SORBS-SPAM, SORBS-WEB, SORBS-ZOMBIE, SPAMCANNIBAL, SPAMCOP, Spamhaus-ZEN, SPAMSOURCES, SPEWS1, SPEWS2, SWINOG, TECHNOVISION, TRIUMF, UCEPROTECTL1, UCEPROTECTL2, UCEPROTECTL3, VIRBL, WPBL, WSFF, ZONEEDIT, CSMA, DUINV, ORVEDB, RSBL, SPAMRBL

And that's not even all of them! There guys can run blacklists out of their mom's basement, and any corporation can have its own blacklist.

Al Iverson has a great article for dealing with blacklists and recommends that the blacklists you want to stay away from are: Spamhaus, SpamCop and UCEProtect. We'd add that its important to pay attention to Barracuda, Lashback, SURBL and URIBL. Also keep in mind that not only are your IPs at risk, but your domain can be blacklisted, red listed or grey listed. Set up monitoring not only for your IPs but also for your domains. Spamhaus will introduce the new DBL soon. It's pretty easy to set up monitoring with most blacklists, and there are many, many scripts publicly available on the web to help you monitor your IPs and domains.

Keep in mind that some of these blacklists will require you to register your IP in order to use their blacklist lookups. Failure to do so could get the IP you're checking from listed as well.

Spam Filters

Spam filters are used by ever major and minor ISP. If it’s not Spam Assassin, it’s a more commercial-grade spam filter. In many cases these filters will catch most, if not all, spam, but sometimes they can be aggressive. Check your content, and test as much as possible.

Return Path offers scanning through a few major spam filters, but you can also do some of this scanning on your end prior to sending campaigns. It’s easy to set up a Spam Assassin install and run your content through it prior to sending, and take it a few steps further by running it through other spam filters or appliances. The difficult part is weeding through the false positives and ensuring that your good content isn't getting flagged as spam. (Sometimes you have to tweak the Spam Assassin rules to suit your needs—just keep in mind some people run default installs of Spam Assassin.)

If you can’t get your hands on the devices used by major ISPs, it’s at least good to know the products used. Return Path provides some information about the spam filters used by the major ISPs. Here are some of the details:

Yahoo uses a proprietary spam filter called SpamGuard; Hotmail, MSN and Live use BrightMail; Gmail uses Postini; AOL uses spam complaints to filter (and if an email receives enough complaints they will block any email with matching domains). Other commonly used filters at the enterprise level are MessageLabs, Barracuda and Forefront. This would affect your B2B email communication, so it’s very important that you keep this in mind. Something else that’s becoming very widely used by ISPs and enterprise/corporate email administrators is content fingerprinting. Cloudmark is a company that specializes in content fingerprinting and has a very high-quality product for helping to detect spam. It’s important to familiarize yourself with the spam filters used, and if possible, it’s great to get these devices into your infrastructure to ensure that you're not sending out content that's going to get blocked.

Seed Lists

In the Deliverability Tools section we touched on the use of seed lists with Return Path's campaign monitor. A seed list is essentially a list of email addresses going to different ISPs (usually multiple email accounts for each ISP), and when you send your campaign, you monitor where the email lands. You don't move, open or touch these emails when they go to the different email accounts in the seed list. It’s important to use seed lists, but it’s also important to not *overuse* them. Since you're not touching the emails, you could potentially cause problems because you're not engaging.

Deliverability Troubleshooting

It’s Not Me, It’s Them

Let’s say some big ISP is blocking your email. The first thing you do is go email them about it right? NO! Don't just start emailing your buddies over at AOL or talking to someone who knows someone. That's NOT what deliverability is about. First start with your infrastructure, your logs, your lists, your content, etc. Not them....YOU. Generally, most issues are on the sending side, and I'd bet that the issues come from crappy engagement, crappy lists or crappy content. If and ONLY if you have those things under control should you engage with the ISP.

I'm Blacklisted

Generally this boils down to bad list etiquette. You can't send commercial email because they verbally told you it’s OK. You can't send commercial email because you bought a list, rented a list, or your vendor said it was cool. There are all sorts of blacklists and different ways to land on them, but all the ways we know of to get listed are due to bad list etiquette. Chances are, you know you're doing something wrong, or your client knows they're doing it. Just do the right thing, unless you like filling out forms and wasting a bunch of time emailing people about how great your list is.

When you get listed, find as much out about the incident that you can from the listing company. Usually they'll at least provide a date and subject line. If you're scraping your MTA logs, you likely caught the incident when it occurred or just after it occurred and can work backwards—similar to working the ISP blocking. Figure out what caused the issue, fix it, and then and ONLY then do you go back to the listing company.

Corporate Domains/Business-to-Business

Remember that corporate domains, small ISPs and international ISPs can employ similar technology as the big ISPs. Corporate domains are sometimes more stringent on rate limiting and spam policies. If you see that you're getting blocked at Bigco's domain or a small ISP, treat it just like you're dealing with an ISP. Get your facts straight, and if they provide any public information for sending, read up on it prior to contacting them.

If you're marketing to government or large non-profit organizations, they would likely be using a Barracuda device, so you may need to get one to check your content. In some cases, these companies might reach out to you for different issues or policy violations. Generally they'll ask you to comply with their standards, and it’s important that you comply as quickly as possible. Some corporations and even small businesses have such strict policies that they might decide to blacklist you if anything looks suspicious. This is why you set up all those email address accounts—so that people could reach out and help you, or alert you to potential issues and possible ways of resolving those issues.

APPLICATION DEVELOPMENT CONSIDERATIONS

Remember that your delivery infrastructure is not just about some servers that are configured with DNS and run an MTA. There's software and code that generally has to be written to handle the construction of the email, constructing pieces of the headers, handling bounces, etc. We've touched on several aspects you need to build into your infrastructure, but we'll summarize some of those and add a few more that you need to consider here:

Agent

Most ESPs have some form of an agent that constructs the pieces of data and email content to pass off to the MTA. Some people opt to have the agent handle merging the data into the template and sending to the MTA for sending. Others supply the data and the content to the MTA and let the MTA handle the merge process.

Merge Data

Most MTAs have some form of merge capability, which allows you to pass in data and use specialized syntax in your content to merge in the data. For instance, if you wanted to start the email with “Dear John,” you could use a merge tag for this data and allow the MTA to handle the processing. This is a widely used feature in commercial email, and you should think about this when you're designing your application and your sending infrastructure.

Also keep in mind that your marketing department or customer will expect to use conditional content to change pieces of the content in and out, depending on say a zip code or a person’s age. All of this can be done with Merge tags, some application code and some commercial MTA products.

Bounce Processing

You'll need to ensure you have some code, script or an intern with lots of time on their hands to process bounces. Using VERP'd header will allow for easy processing, but remember to include enough data in the VERP'd address to be able to find the contact and remove them from the list.

Click Tracking

If you want your marketing team or customer to understand who's clicking on the links in your email, then your applications need to be click aware. Allowing some capability for your users to understand who's clicking and which link they're clicking is vital. This is delivery-related because you want to track these stats and understand how subscribers are engaging with the email.

Email Headers

It's important that your code or your MTA is set up to allow you to pass in custom headers. You want to include a VERP address, Unsubscribe link, abuse contact information and other unique identifiers. If you're using commercial monitoring tools, most of them will require some use of a unique identifier in the headers. Consult with the monitoring tool company and your development team to determine the best header option. Keep in mind that you can provide multiple headers to uniquely identify your email, but also remember that bounces and FBL emails may not always contain this data, as there are no set standards.

FBL

Again, you'll need some code, script or an intern to process FBL requests. Just keep in mind that the data can be munged, and some headers may not be intact. Make sure you get notified when an abuse complaint fails to process. Whatever you do, don't go live without this, and register with ALL ISPs for all your domains and IPs.

Open Tracking

Similar to click tracking, you should be able to offer some form of open tracking. The industry standard is generally a 1x1 pixel image that's embedded in the body of the email. When the user has images turned on, the open is recorded. This is important just like click tracking, because you want stats on list engagement metrics.

WHAT IS DELIVERABILITY?

We've mentioned the word deliverability quite a bit in the document, so we'll leave you with some information about the soft skills and human side of your delivery infrastructure. Deliverability is both an art and a science that ensures an email reaches its intended recipient. It's more complex than it seems, though. Deliverability is a maze that's navigated by learning the expectations of ISPs, monitoring statistics, building a solid infrastructure—and of course, a whole lot of trial, error and patience.

Your infrastructure and content have a reputation with each ISP, and as the deliverability genius, it's your job to maintain that reputation. When deliverability goes wrong, you can find yourself on blacklists, getting heavily bulked, and having to explain to your CEO why his *email marketing blaster cannon thingamajig* isn't working. Failing to monitor and secure your delivery infrastructure is a silent killer to the effectiveness of email marketing. With the new systems being put in place by ISPs, the deliverability and reputation of your company will become even more important—and with that responsibility on your shoulders, you want the best possible infrastructure in place.

The good, the bad and the ugly

If you follow the steps outlined in this guide your email marketing cannon will see far better inbox placement, your CEO/marketing team will pay you 10 cents more an hour and will put you ahead of your competition. So what's the worst that could happen if you ignore this stuff? ISPs can choose to block you. Not a 24-hour block or a "fix issue A and we'll allow you to send to our users again" temporary block—they'll block you indefinitely or give you a "come back in nine months when you've cleaned up your act" response. You could also land on blacklist after blacklist, filling out forms and working overtime to fix the problems. Not to mention, people will directly complain and report your email as spam. Trust me—it's not pleasant. Without putting in place all the technology and manpower mentioned in this guide, you may not know there's a problem until it's too late. Once administrators start sending you emails to notify you that you're blacklisted (if they're nice enough), there's not much you can do.

Now that ISPs are moving to an engagement model, entire domains will often get blocked from sending, and simply getting email delivered will be much tougher. Properly building your infrastructure will put you ahead of the curve.

Deliverability Team

Team? What do you mean? It's just me!

Working on your own is perfectly fine, but we use the word "team" because you'll have to wear several hats. (Note that if you plan on doing this delivery thing on a large scale, it's probably going to take more than just you.) The first order of business is planning out the responsibilities if you have a team, and if you don't have a team, mapping things out so that you’re not stretched too thin.

ISPs, email administrators, subscribers and other contacts need a way to communicate with you. Generally, all ISPs, email administrators and anti-spam authorities will communicate over a series of expected email accounts. You have to set up email addresses to allow people to contact you with issues or questions. *You should at minimum have an abuse@, postmaster@ and fbl@ address for people to get in touch with you.* Most ISPs will expect some of these to be set up to register for FBL, whitelisting, etc. It’s important to do this up front and get it right, as changing this data can be close to impossible once you're up and running. Even if you want all this to go to one address, set up each address and forward it to one inbox—don’t go down the tempting route of setting up one catch-all for everything.

You should also think about growth. If you do grow out of that one-person team, you want to be able to easily move the responsibility of one or all of these inboxes to a new hire. It's vital that these email accounts have spam filtering, as they're common addresses, so they'll receive lots of unwanted email. If you're using multiple domains or aliases, it’s a good idea to ensure each domain and the aliases associated with those domains have these email boxes and properly forward:

postmaster@

This is a common address with domains. It *can* be a catch-all, but for some registration-related stuff, it may be needed. Someone receiving unwanted email will likely try to file a complaint or a question to this address. If you have multiple domains, set up this mailbox for each sending domain.

abuse@

This address is a must-have. It's used for handling direct complaints from subscribers, ISPs or other permission-related issues. Sometimes your hosting facility will use this address if they see issues with your content or receive complaints directly. If you have multiple domains, set up this mailbox for each sending domain.

fbl@

In order to process abuse complaints, you need to set up your feedback loop process and have the ISP or email administrator deliver to your fbl@ address. You want this address to only receive fbl email, or make your fbl process smart enough to only process fbl requests.

alerts@

We'll discuss alerts a little later, but be sure to have an inbox that collects your alerts. These may be triggered alerts, MTA errors or monitoring alerts.

Hotmail, Yahoo, Gmail, etc.

Set up an email account with each major ISP or email system. You can set up two different types of accounts or combine them all into one, but we recommend one account for testing purposes, and another for support/tools/postmaster-related stuff with those sites. Hotmail SNDS requires a hotmail account, and Yahoo requires accounts to register FBL. Don't use your personal accounts for this, as you don't want to have to go through changing ownership over if you leave your post.

TERMINOLOGY

You may want to become familiar with these deliverability terms:

Abuse Complaints

Abuse complaints occur when a subscriber clicks "Report Spam" in their email client. For ISPs that use feedback loops to report abuse complaints, you can record these abuse complaints and unsubscribe the complaint. It's important that abuse complaints are removed, because failure to remove a complaint is a common reason for ending up on a blacklist.

Blacklist

Lists maintained by companies that specialize in revealing IPs or domains that are either sending unsolicited email, engaging in bad email practices or associated with a website that's engaging in bad practices. There are multiple blacklists, and some are more serious than others. Some ISPs maintain their own blacklists, which consist of public blacklists and their own internal blacklists based on engagement or direct complaints.

Bulking

Bulking occurs when the email is routed to the spam folder instead of the inbox. Bulking can occur because you're not using authentication, your content has spammy keywords or resembles spam, or something in your infrastructure's history is causing concern.

Dedicated IP

The use of an IP for one client or department’s traffic. No other traffic is sent over a dedicated IP.

Direct Complaint

A direct complaint occurs when someone reaches out directly to your domain by either replying to the reply-to address or your abuse@ email address and complains that they no longer wish to receive email from you. It's generally best to just unsubscribe them and let them know they're unsubscribed. Don't ask them to do anything, don't beg them to stay, etc.

Engagement

Engagement refers to how your subscribers are responding to the content that you're sending. Are they regularly opening your email and clicking on your links? If they're engaging with the content, your reputation and deliverability will improve. If they're not engaging with the content and are deleting, marking as spam or unsubscribing, your reputation will drop and affect your overall deliverability.

Feedback Loop

A feedback loop (or FBL) is a process wherein the recipient clicks "Report Spam” in their email client, and if you're registered with the ISP’s FBL process, they'll send you a specially formatted message that says who complained so you can unsubscribe them from your list.

ISP

Note that an ISP can be a corporation or anyone receiving email. Don't just assume that ISPs are the only ones capable of implementing technology to filter your email, provide FBL reports, etc.

MTA

An application or piece of software responsible for transferring or routing email from point A to B.

Reputation

Reputation refers to how an ISP views your content and/or infrastructure. ISPs track your reputation either by domain or IP. It's like a grade in school. That grade is tied to your IP or domain and determined by algorithms that differ with each ISP. Generally, the reputation is determined by some formula of engagement, abuse complaints, bounces and send volumes.

Seed List

A list that consists of email addresses with the major/minor ISPs that's injected into the campaign to see where the email is delivered. You don't touch these emails in any way—you just want to see where the email is placed or if it’s delivered at all.

Shared IP

The use of a group of IPs used for multiple clients. All of the traffic is spread across multiple IPs because the volume or traffic is not appropriate for a dedicated IP.

Spam Trap

Addresses that have gone stale or are old that ISPs have turned into honeypot addresses for catching senders that are engaging email accounts without permission. Generally you'll see spam traps in old lists, purchased lists or lists collected improperly. The best way to get rid of spam traps is to use reactivation or pruning techniques with your list on a regular basis. (And, of course, to use strictly permission-based lists!)

Subscription, Subscribe or Subscriber

A person who has given you tangible and confirmable proof to engage in sending them commercial email.

Unsubscribe

A process in which a subscriber requests to be removed from a list. You're required to honor all unsubscribes, and failure to process an unsubscribe is a violation of CAN-SPAM.

VMTA

Some MTA applications will allow you to set up a virtual MTA that allows multiple MTAs to run on one machine, all using different IPs and domains. So instead of having five machines for the five sending domains in your infrastructure, you can have one machine that has the MTA configured with five (or more) virtual MTAs.

Whitelist

A list or registry of approved senders. Note that being on a whitelist doesn’t mean you can violate terms or build a poor reputation. Doing so will get you booted from a whitelist.