



RocketMail
Powered by 10Fold Solutions

Understanding Email Deliverability
A Guide To Best Practices In Email Marketing

Introduction	3
The Basic Delivery Model	4
1 Assemble the Right List	5
Subscriber Consent	6
Spam Traps	10
List Segmentation	11
Targeted Content.....	11
2 Create Great Content	11
noreply@ Email Addresses	14
3 Transmit the Message Cleanly	15
Sender Reputation	15
4 Deal with Recipient Issues	18
Junk Mail & Spam Complaints.....	19
Soft & Hard Bounces	19
Transmission Rates & Errors.....	20
Email Client Spam Filters	20
Messages Deleted By Recipients	20
Recipients Unsubscribe from Future Messages	21
5 Track the results	21
6 Manage list hygiene	22
7 Fine-Tune Content to Maximize Engagement	22
CAN-SPAM Compliance.....	22
The Big Picture.....	26
Other Useful Resources:	27
About RocketMail.....	Error! Bookmark not defined.

Introduction

Getting your email marketing messages to your target audience is about more than just writing an email and hitting send. It's a complex process that relies heavily on reputation, valuable content that engages recipients, a contact list full of subscribers who want to receive your email and a skilled interactive marketing delivery platform to get it there. The most important part of this equation is the reputation you have acquired by the practices you adhere to as a sender. If you take nothing else from this paper, know that you have to *earn* a positive online reputation, but once you do it can make the difference between your email getting delivered to the Inbox, junk folder, or not showing up at all.

This RocketMail white paper looks at the best practices in email deliverability - arming you with the facts in plain English and giving you a list of criteria for successful email marketing campaigns that ensure they get to your audience's inbox. Most of what you'll learn amounts to a single golden rule: **send interesting & valuable content to people who have agreed to receive it.** We also cover what's required under the law, how to build great lists, how to develop great content and what happens (and what you need to do) after you hit send. This information is crucial to developing a good reputation with your audience, ISPs, and anti-spam organizations.

At its simplest, successful email delivery consists of seven basic steps:

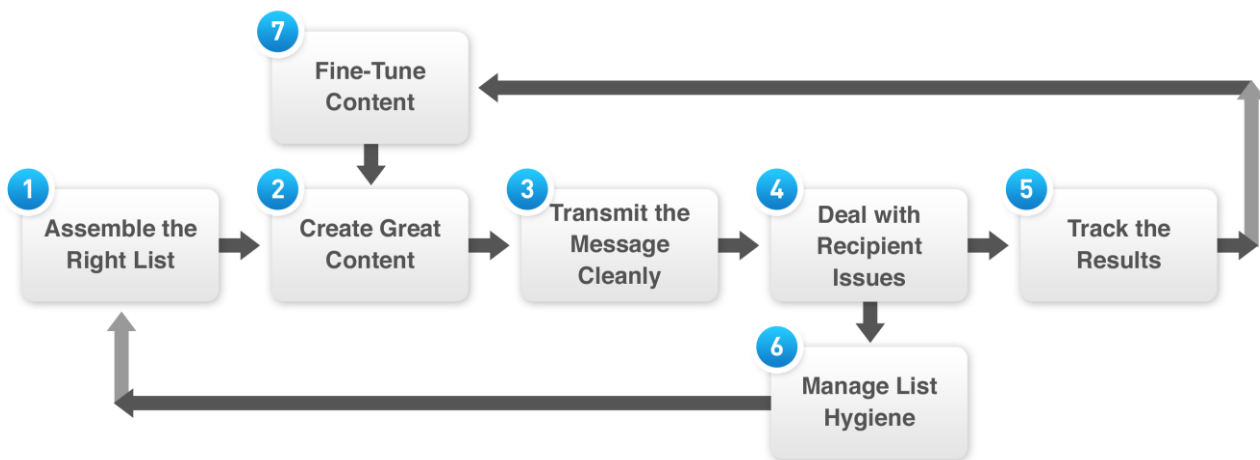


Figure 1: The seven steps of successful email marketing

The Basic Delivery Model

1. **Assemble the right list**

The ideal audience wants to receive your email, has given you consent to email them and most important, is expecting you to send it. The list you send to should be targeted at a specific segment of your market, and it **must** contain accurate, current contact information. Generally speaking, this list will be an audience you've grown over time.

2. **Create great content**

No marketing campaign can be a success if the content isn't well written, compelling, and of value to the recipient. You know your audience best; now share content with them that they'll want to read and keep them engaged.

3. **Transmit the message cleanly**

This means respecting delivery rates and complying with ISP guidelines - ensuring that the maximum number of messages reach your recipients' inboxes. These—and many other—factors govern your reputation as a sender. The more credible and legitimate you are, the more likely your messages are to reach their intended destination.

4. **Deal with recipient issues**

If an ISP thinks your email is spam, they will defer or block it very quickly. If an individual thinks your email is spam (or doesn't recognize you) they will flag your email as spam, which registers a complaint. Both of these issues can harm your reputation and should be dealt with quickly and fairly.

5. **Track the results**

Every campaign has success rates that you can learn from, particularly if you're testing several messages against one another. Results of each campaign allow you to compare success over time and discover trends in both your content and the behaviour of your list that allow you to better tailor your future content and messages.

6. **Manage list hygiene**

Recipient issues such as complaints, unsubscribes, and hard bounces should update your list immediately to ensure that it remains clean. Emails that soft bounce repeatedly should be removed from the list, as should people who have not registered a click or open for the last few mailings. At the very least, you should send an email to those who haven't opened your emails or clicked links recently asking them to confirm that they wish to remain on your list.

7. Fine-tune content

The results of a campaign should lead to improvements in future messages - meaning that you're constantly optimizing what you send in order to maximize the outcome.

Of course, each of these steps is far more detailed than just what's included in the list above. Some of the steps are the responsibility of marketers, while others are the job of an email marketing platform. The following pages break each of these steps out into more detail.

1 | Assemble the Right List

Every marketing campaign begins with an audience, which is who your message is tailored to. Of course, you can't send messages to just anyone—you need interested recipients on your lists that have opted-in or have given their consent to receive messages from you. Without the right consent from your subscribers, the email you send them can only be classified as spam.

The right list has to follow specific rules of hygiene:

- **It must have appropriate consent.** Recipients must have agreed to receive your message, either because they opted in to a mailing list, signed up for a newsletter, or agreed to get content from you.
- **It must be up to date.** People's email addresses can change, and you need to send to their current address. If an email bounces because the address is no longer valid, it must be removed from your list.
- **It must respect a recipients right to change their mind.** If someone has opted out of a mailing list, they must be removed and not receive another message.
- **Ideally, you should be whitelisted by recipients.** This means that the recipients email server and mail client should know that emails from you are legitimate no matter what content you are sending them. You should encourage recipients to add you to their contact list, address book, or to their approved sender list to alleviate content filters issues and help establish you as a "trusted" sender. Most ISPs provide their users with several ways of doing this. For example, if the user clicks any of the following after opening your email: mark this sender as safe, enable images from this sender, never send email from this sender to my spam folder, add sender to my contact list, etc.

Having an existing business relationship with someone doesn't mean it's okay to add them to your mailing list. If you are adding people automatically, or the sign up process isn't clear, many of your recipients will flag your email as spam simply because they don't recognize you or didn't want your email to begin with.

Complaints are the **number one** influence on your reputation so it is in your best interest to do everything you can to avoid recipients clicking the spam button. To avoid complaints you should:

- Never use a purchased, harvested or "scraped" list of any kind
- Make sure you have a direct relationship with every single address on your list
- Start confirming new signups (using a confirmed or double opt-in process)
- Ask people if they want to be on your mailing list. DO NOT sign them up automatically
- Make your signup process clear, explaining what someone is signing up for, when they will start receiving emails, and how often they can expect to hear from you
- Use a consistent From name and email address
- Use a subject line that truthfully describes the content of your email
- Honor all opt-out requests immediately
- Abide by the rules of CAN-SPAM
- Keep your list current and up to date
- Don't reactivate old addresses
- Send emails on a regular basis

If you comply with all of these rules, you're off to a great start. To make things even better you'll want your list (and the messages you send to them) to be both segmented and your content to be well-targeted.

Subscriber Consent

The best mailing list is one filled with recipients who've explicitly requested that you send them something, but there are many kinds of mailing lists used in the industry, classified according to how reliably the recipients have indicated their willingness to be contacted:

- **Confirmed "Closed-loop" Double Opt-in**

When someone signs up for your mailing list, a confirmation email is sent to their email address and an action is required (like clicking a link) in order to confirm that the address is valid. It is highly known throughout the industry as being the most effective method of growing your list as only the true owner of the email address can sign up and confirm their subscription - therefore generating very few complaints, if any. It also prevents you from adding any invalid and/or spam "trap" addresses to your list as they will never complete the confirmation process.

- **Notified Opt-in**

This type of opt-in sends a Welcome email to new subscribers upon sign up, but does not require any additional confirmation from them in order to be added to the list. This type of opt-in is a popular method, though it can be prone to abuse and lead to lists with more complaints than a two-step Double Opt-In process.

- **Single Opt-in**

Single opt-in is when someone knowingly signs up to a mailing list by checking an empty "Yes, please sign me up to receive news from company x" box when submitting a form (like an online shopping cart, or account registration for a particular website). Although better than the Opt-Out method we'll talk about next, this method leaves list owners open to abuse and generally results in a higher spam and/or Bounce rate that can lead to serious delivery problems.

- **Opt-Out (Implied consent)**

Opt-out list building occurs when an email address is added automatically and users are required to either unsubscribe upon receipt of an email or to uncheck a box when submitting their data on a form, or as part of a checkout process. Using Opt-Out methods as a way to build your list is a bad marketing practice and can make recipients feel as if they were tricked, damaging your relationship and reputation in the process. This method typically generates a large volume of emails flagged as spam which negatively affects your reputation as a sender and in turn your delivery rates.

- **Affiliate Lists**

Affiliate lists are the results of one company sharing an email address (or a list of addresses) with other partners or affiliates. If a person signs up to receive email from Company A, they should only receive emails from Company A. If they also receive email from Company B, because they signed up with Company A, they are more likely to complain. Often this will appear during a signup process as something along the lines of "Yes, please send me information from Company A *and relevant partners*".

- **Purchased Mailing Lists**

Purchased Mailing Lists are lists of email addresses that have been bought from someone else for a price. Many companies contemplate buying lists as a means of building a mailing list quickly, but **consent is not transferable** and these types of lists are a marketing worst-practice. Not only have subscribers on that list **not opted in** to receive emails from you, they are likely going to flag your email as spam, and you have damaged your

marketing relationship with the receiver before it has even started. This will also directly affect the delivery of your existing clients that have opted in to receive these mailings.

- **Rented Mailing Lists**

Rented lists are similar to purchased lists, in that the sender has no relationship with the intended recipients and are usually used for a one-time mailing to help grow your list quickly. Often the marketer never sees the list, but simply provides the content and is at the mercy of the list owner to send the message on their behalf. This can result in a high bounce and/or complaint rate and the reputation being tarnished is shared between the list owner and YOU (the sender). The recipients may also learn that you're adopting bad marketing practices.

Regardless of who sends the email, if the content is yours, you're responsible for what others do on your behalf: the Federal Trade Commission (FTC) says that "even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law."

- **Harvested Lists**

This technique is employed by spammers who acquire email addresses by harvesting or "scraping" them off the Internet. They search for anything that resembles a valid email address (like something@domain.com) or run Directory "Dictionary" Harvest Attacks that find valid addresses using a process of trial & error. These attacks are more effective for finding email addresses of companies since they are more likely to have a standard format (i.e., jdoe@company.com, johnd@company.com, john.doe@company.com). No one on a harvested list has opted to be there or has a pre-existing relationship with the sender. It goes without saying that harvested lists generate a high volume of complaints, a lot of bounces and very poor email deliverability.

Important Note:

Using a Harvested, Purchased, Rented, and/or Affiliate list is a bad marketing practice and a violation of the RocketMail Anti-Spam Policy.

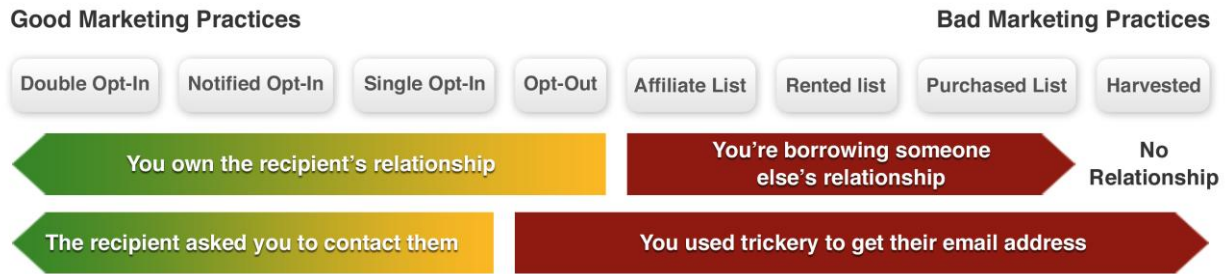


Figure 2 shows the various degrees of list quality based on how lists are acquired.

Spam Traps

Spam trap addresses are addresses that may or may not exist and are used to judge your sender reputation. The term “trap” is very appropriate in that these addresses are scattered throughout the internet to catch people either not using proper list building practices, harvesting emails, purchasing lists from a 3rd party, or marketers who have poor list hygiene (whether they know it or not). These trap addresses are kept secret to protect their identity and are released to no one because making them public would render them rather useless.

There are two types of spam traps:

“Honeypot” or “Planted” Traps:

These email addresses have been intentionally created to trap spammers searching the millions of websites on the Internet for any address they can find. These traps are never published and do not belong to a real person thus could never “opt-in” to any list since it is impossible for the address to initiate, respond or give consent to having received email of any kind. Sometimes referred to as a “honeypot” or “planted” address, they are used by anti-spam groups to catch spammers, monitor and collect spam. If you send an email to one of these traps, you **will** get exposed for using illegal marketing practices and you **will** get blacklisted which will seriously harm both your delivery and your reputation.

“Dormant” Traps:

These are usually addresses that have been deactivated for a period of time (as little as 6-12 months) and are used by ISPs to judge the quality of your list data. These addresses no longer receive email except to catch this sort of activity. Sending to a “dormant” trap address will not usually result in being blacklisted because these addresses may have opted in to your list at some point. It does, however, raise flags because you are sending to an email address that is out of date and indicates that you may not be processing hard bounces correctly and/or not removing them from your list. Sending to dormant addresses at any one ISP **will** affect your delivery.

What can you do?

- Stop using purchased, rented or affiliate lists
- Start confirming addresses for new subscribers with a double-opt in process
- Keep your lists up to date
- Send emails to your list on a regular basis (at least once every six months)
- Make sure you are processing hard bounces correctly*

* When changing providers, make sure you do not reactivate any hard bounces or unsubscribes from your current list. Addresses that have previously been marked as invalid could potentially be turned into trap addresses and sending to someone who has opted out is illegal.

List Segmentation

While it may be tempting to build one list and email them all with a single message, there is tremendous marketing value in using a segmented list. Segmenting refers to creating small groups out of a larger one – so taking your one big list and turning it into a number of smaller lists based on certain criteria. The criteria could include demographics (age, gender, education or others) or could include things like buying behaviour, memberships, or any data that users submit when subscribing to a list, what pages they visited on your website, what they clicked on and more.

Once you have this sort of data in a large list, it's easy to create categories of subscribers. While you can still email the full list with a single message when merited, you can also now send an email with targeted content that appeals directly to certain segments of your audience. Do you want to send an email to just the women on your list, not the men? How about those that made a purchase within the last six weeks? Segmentation makes that possible (and easy, too).

Targeted Content

Innovations in email marketing give you more power than ever before to send targeted, personalized and better yet, dynamic emails to list members. The more specific and targeted your message is for your recipients, the more likely you are to see success in your campaign results – whether you measure results in opens, click-through, or even revenue generation.

With RocketMail's new Dynamic Content abilities, it's easy to create targeted content and send messages in multiple languages, or alter the message based on how long someone has been on your list, what their personal preferences are, or based on past behaviors like opening or clicking on links in previous emails you've sent them.

2 | Create Great Content

More than anything else, great email content engages and informs the reader. It should also encourage the recipients to open your message. Something as simple as using a short, intriguing subject line or familiar term will entice them to want to read more and gives them a clear indication of what to expect.

In addition, great content also follows certain guidelines:

- **Watch Your “Spam Score”**

Most spam filters, whether they are desktop software or server-based, use a set of keyword searches to determine whether a message is spam. Using words like sale, credit, casino, or free can hurt your deliverability, but sometimes it’s hard to predict on your own what will trigger a spam filter. Lucky for you, there are tools that will warn you if a message is likely to wind up in the junk folder or be flagged as spam. RocketMail customers can make good use of tools like Litmus, which allows you to test and adjust spam level scoring before you hit send, and also allows you to make sure that your email campaigns look great across different email clients, browsers and mobile devices.

- **Personalization is Key**

The more a recipient knows the message is directed at them, the more likely they are to open and read it. Personalization of content is one of the most significant factors driving interactive marketing conversion rates. It may be as simple as a “Hi Joe,” instead of “Hello Customers,” or can be much more sophisticated such as “Happy Birthday Joe!”

- **Reflect your brand, and reinforce it**

You want your recipients to know that the message is from you—not from a third party. If a recipient doesn’t recognize you (the sender), they are more likely to unsubscribe. Worse, they may flag your message as spam, making it harder for subsequent messages to reach those who want to receive it. Ensure you always reflect your brand well with legitimate “From” names and a valid reply address that is managed by a real person. The domain used should also have functioning abuse@ and postmaster@ addresses as well as public WHOIS information. Use custom templates that include your logo or other recognizable images that will make sure your recipients know it’s really you.

- **Comply with the law**

The CAN-SPAM act defines the essential requirements of what email messages need to contain, and you must follow those rules. For example, your messages must have a working opt-out/unsubscribe mechanism, and include a physical postal address of the sender. See the section later in this document on ‘CAN-SPAM Compliance’ for a complete list of requirements.

- **Watch your HTML**

If you are sending messages in HTML, your code can also get you flagged as spam. Avoid using image names like “free.gif” and always use alt-text to provide context when images are not displayed. Most email clients today do not display images unless the recipient has deemed your email to be safe or wanted by clicking “Display Images” or “This is a Safe

sender". Excluding images can make emails pretty boring to look at, so the ideal solution is to take care with how you name them and always have a good balance of images and text.

- **Choose Your Formatting Wisely.**

You wouldn't use **huge fonts**, **bold** text, third-party links or use ALL-CAPS in a message to a friend. Doing so in your marketing emails can make these messages look like spam rather than what you've intended them to be. Emails are like any other creative piece and should be designed strategically for each recipient.

- **Clear & Concise Subject Lines**

Your subject line should be a compelling short piece of content that prompts your recipients to open your email and read more. This is particularly true if your target audience uses mobile devices, where screen real estate is at a premium. Most iPhones display about 30 characters in a message title, while most Blackberry devices show only 15.

Your marketing message, along with these guidelines, makes up the content of a campaign. Content may be a single message, or it may be a series of messages (such as an ongoing newsletter or a drip campaign). If your communications with your audience will be recurring, then they should involve a standard structure – recurring content themes and consistent branding - with which they will become familiar and trust.

Like any marketing tactic, competitive and market research can provide you with ideas about what works with particular markets, creative inspiration, and even occasionally, some great don't-do-that moments. Signing up to receive emails from your competitors and for best-in-class newsletters from others can be a source of inspiration and give you great ideas about how email marketing can really be done well.

Lastly (but definitely not least), make sure you're using the right language and terminology, and you've double-checked spelling, grammar and punctuation before you hit send.

Included below is a quick checklist of things to keep in mind when you're preparing your campaign:

- Avoid using 'spam' words (credit, casino, free, etc.)
- Make sure there are no spelling or HTML errors
- Avoid using ALL-CAPS in your content
- Keep the use of multiple exclamation points (!!!), question marks (??) or symbols like @ \$ # to a minimum
- Make sure your text version matches your HTML version
- Try to keep **bold** type to a minimum
- Keep your text to image ratio around or below a 1:1 ratio (minimum one paragraph of text

- for every image)
- Keep Subject lines under 25 characters in length (including spaces)
- Make sure your Unsubscribe link is visible in plain text
- Always use ALT text for images
- Avoid using background images whenever possible

noreply@ Email Addresses

While the From name and email address might seem like small details, they can make a huge difference to the success of your campaign. By sending an email with a From address such as 'noreply@domain.com' or 'unmanned@domain.com' you are sending a message to your customers and it's "Please don't talk to us".

"From" addresses like noreply@ that (a) aren't manned by a real person or (b) don't exist at all can be an easy way to alienate your customers and eliminate feedback from your users. If you send your email from a noreply address, here are a few reasons to make the switch to something new (like an email address manned by a real person):

1. Your email is more likely to be flagged as spam or deleted by the recipient.
2. The message you're sending to your subscribers (those current or potential customers) is that you're not interested in receiving their email, even though it's ok for you to email them. Is that really the message you want to send?
3. You're missing great (and sometimes crucial) customer feedback – user comments, unsubscribes – that can help you improve your marketing efforts (and see more return on investment).
4. When someone replies to your emails, you're likely to be automatically added to their contact or "Safe Sender" list at the same time which means all your future emails you send them will go straight to their inbox. Replies should be encouraged!
5. Modern webmail & mobile email clients show people more than the name of the sender – they show your email address as well. Would you open email that was from noreply@domain.com?
6. Using a noreply@ address has been shown to decrease open rates, increase unsubscribe and complaint rates.

Not convinced? Check out what the pros have to say about it:

The CAN-SPAM Act: A Compliance Guide for Business

“Your “From,” “To,” “Reply-To,” and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.”

MAAWG Sender Best Communications Practices:

“Senders should have the capability to process email-based unsubscribe requests. Senders should also consider making offline unsubscribe mechanisms available. The sender’s ‘From’ or ‘Reply-to’ email address should also be able to receive unsubscribe requests, unless otherwise indicated.”

3 | Transmit the Message Cleanly

Once you’ve written great content, designed a beautiful email, tested it and directed it at a targeted, segmented mailing list, your work as the creator of the campaign is done. Now, it’s time to send your message!

The point at which you hit Send is really where a robust email marketing platform, like RocketMail, becomes absolutely essential. There are many obstacles your message needs to overcome between when you hit send and your recipient opens and acts on it. Assuming that the content is legitimate and the recipients are valid, it’s the email service provider’s job to send it.

Sender Reputation

As a sender, you’ll gradually acquire a reputation as you send messages over time. The combination of your content, how often recipients flag it as junk, spam traps, and your bounce rate all contribute to this reputation. A good reputation has a great impact on the effectiveness of your marketing efforts. A bad reputation does the exact opposite and may prevent it from reaching your audience at all.

Cultivate and nurture your reputation by practicing good list hygiene, sending valuable content, and keeping your audience engaged. **A solid sender reputation is an important asset – without it reaching your audience can be a significant challenge and will inevitably impact the success of your campaign.**

Most receiving networks use several factors to judge the reputation of a sender. Some of these are within the control of the marketer or sender, and others need to be managed by your email service provider. They include:

Managed By Marketers

- **Complaints**

This is the rate of formal complaints, or the number of recipients marking messages as spam. Avoiding complaints relies on sending quality content to subscribers who have opted-in to receive your emails. For a more complete list of things you can do to avoid complaints, please refer to the “Assemble The Right List” section on page 5.

- **Hard Bounces**

The hard bounce rate is the percentage of emails you send that are sent to expired or inactive addresses. This can be managed by maintaining an up-to-date subscriber list and ensuring it’s easy for people to unsubscribe or modify their information when their contact details or circumstances change. ISPs monitor hard bounces very closely and significant hard bounces can impact your campaign’s (and future campaigns) deliverability.

- **Spam Trap Hits**

This indicates how many of your messages are delivered to a spam trap. Spam Traps are email addresses intentionally designed to identify spammers that are harvesting addresses off the Internet and/or senders who have poor list hygiene or opt-in practices. To avoid this, make sure your opt-in process is a double opt-in list that requires people to confirm their email address before they are added to your list and send on a regular basis to remove any invalid addresses that might eventually be turned into traps.

- **Spam Score**

This is the element of email deliverability over which marketers have the most control and yet it’s often the most neglected. What matters more than words that might flag spam filters—which can be avoided—is bad content that encourages the recipient to delete your message, opt out of future messages, block you entirely, or worst of all complain to their ISP by flagging your message as spam.

- **Sender Compliance**

This is measured by how well you adhere to the above requirements. Each mark against you will affect how your future email is handled. How each ISP deals with this can be different - some have higher thresholds than others so you need to stay compliant in all areas in order to keep out of trouble.

Managed By Your Email Service Provider

- **Technical Compliance**

Better known as RFC (Request for Comments), which is a set of standards for the internet as decided on by the [IETF](#) (Internet Engineering Task Force). At a high level, RFC compliance is solely the responsibility of your Email Service Provider and without it most (if not all) of your email would not make it very far.

- **Authentication**

Because spammers often masquerade as legitimate senders (claiming that their emails are coming from a real company) receivers will often look to authentication as a way to see if the sender is really who they say they are. This is especially important when using an email service provider as they may (or may not) be allowed to send on your domain's behalf. There are four main protocols in use today (SPF/Sender ID, Domain Keys and DKIM), but because none of these protocols are dominant, any reputable email marketing platform will make all available to their clients in an effort to help maximize delivery.

- **Accreditation**

Some senders get approval from anti-spam organizations and 3rd party Reputation Providers for certifications such as *Goodmail*, Return Path's *SenderScore Certified* and the *Habae*s Safelist. This means they are pre-approved or 'whitelisted' senders and the ISPs that use these Accreditation services will give preferential treatment to these senders by allowing more email to the inbox and quite often it will by-pass more heuristic forms of spam filtering such as content filtering, throttling or disabling links/images by default.

- **Blacklists**

A blacklist is a list used by receiving networks to judge a given IP and/or sending domain's reputation. These lists are run by anti-spam groups and most blacklistings are the result of sending Unsolicited Bulk Email (UBE) to addresses that never asked for it. There are many different blacklist providers in existence and some carry more weight in the community than others so it's very important you keep your lists clean or you will run into trouble.

- **Whitelists**

Similar to accreditation where reputation is acquired by the means of an outside source, many ISPs maintain their own internal whitelists as well. They are made up of IP addresses or domains that generate very few complaints, bounces and have a high level of engagement with their users. This can also be done by a recipient adding your From address to their Contact of 'Safe Sender' list or going into their Junk folder and telling the ISP your email is NOT spam.

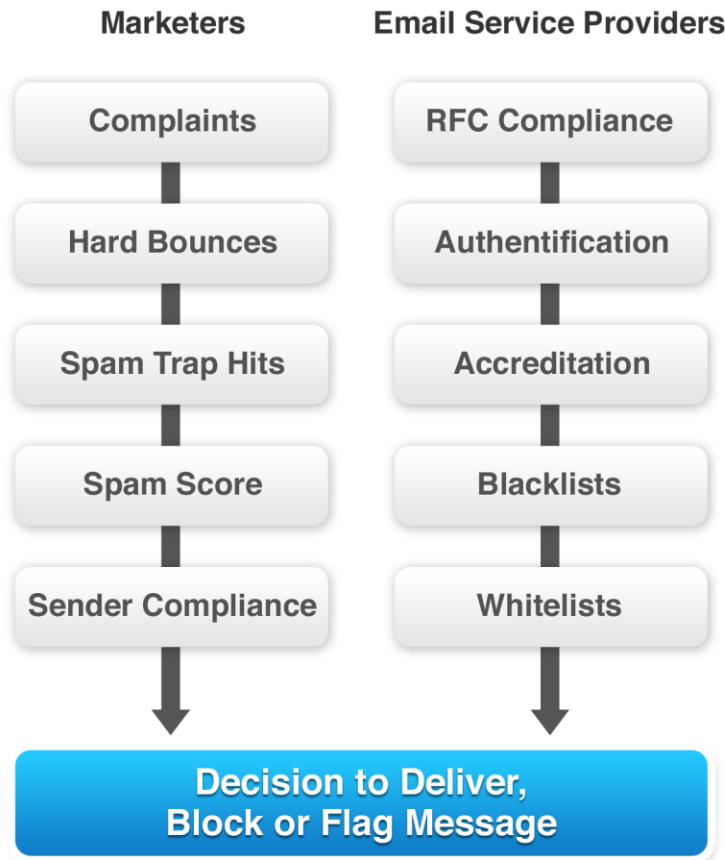


Figure 3 above shows these many factors and how they contribute to an overall decision about whether or not to deliver your message to the intended recipient.

4 | Deal with Recipient Issues

The first step in fixing a problem is to pinpoint what's causing it. A good email marketing delivery platform is able to distinguish between different kinds of recipient issues, so the provider can easily determine whether it's a transmission issue, list/content issue or due to poor sender reputation.

Many delivery issues can be resolved by quick intervention by the email marketing service provider on your behalf. In some cases, there's nothing the service provider can do to remedy the situation – like when email addresses are invalid or when recipients choose to unsubscribe. This is one of the reasons that interactive marketing is more than just software: it sometimes takes human interaction to work through a delivery issue.

A number of obstacles can prevent or slow down your email in between. Here's a look at some of them:

Junk Mail & Spam Complaints

Recipients who flag your mail as "Spam" or "Junk" have the greatest impact on your reputation as a sender. It is essential you avoid this at all costs by delivering great and relevant campaigns to recipients who want to receive it.

Users can (and will) complain about your message and flag it as spam if they have asked to be removed unsuccessfully, if your content isn't of interest to them or if you are emailing them without permission, to name a few. This may be as simple as clicking the "Flag As Spam" button, or it may even involve forwarding the message to an authority that can take legal action. At the very least, messages being flagged as spam will tarnish your reputation, but may also have financial or legal repercussions which could also get you (or your domain) blacklisted.

A recipient marking your email as spam will move your messages to their junk or spam folder, but it also tells their provider that messages of this sort—from this sender, about this subject, from this IP/domain—are more likely to be junk and unwanted which affects how future email sent to that provider is handled.

If somebody wants to unsubscribe from your list, they are going to do it anyway, so you should always **make it easier for them to unsubscribe than to complain**. If your email is long, it is best to insert the unsubscribe link at the top of the email rather than all the way at the bottom (or include it in both locations). The worst thing you can do is make it difficult for subscribers to figure out how to unsubscribe.

Soft & Hard Bounces

A "soft" bounce is a transient error—sometimes caused by the recipients mailbox being too full but can also be caused by greylisting, server timeouts, network congestion, domain/IP based throttling,

and more — that does not result in the removal of the recipient from the mailing list but may temporarily delay delivery to that person. Your delivery platform will retry delivery several times before pronouncing the recipient unreachable.

A “hard” bounce is an undeliverable message resulting from an email address or domain that is determined to be unreachable after a single attempt. These unreachable addresses are considered to be “Invalid” and will be removed from your mailing list. Email addresses and domains often change or expire – whether they are because of people changing jobs or domains expiring, occasionally recipient information may no longer be valid. Addresses may also be entered incorrectly when people subscribe for your mailing list if you use a single opt-in or manual/offline opt-in method.

This issue can be minimized by validating email addresses and keeping your list ‘clean’ through double-opt-in confirmations on sign-up, giving users the ability to edit their subscription information (and thereby update their email address if it changes), and by maintaining frequent communication with your subscribers to ensure the list is as up to date as possible.

Transmission Rates & Errors

One of the things a good email service provider manages for their clients is the rate of network traffic. It sounds odd, but it’s important to make sure you are not sending too much too fast as this can trigger blocks or otherwise raise an alert with ISPs that there is a sudden increase in traffic (this is especially true of IPs with little or no sending history). These flags can lead to timeouts, throttling and even blocks, damaging your reputation in the process.

Email Client Spam Filters

Even if your message has made it to your recipient’s mail server, a client-side spam filter may still prevent it from reaching their inbox. While server filters block out egregious spam, client-side filters are more personalized. Some email clients build their own profile of blocked senders and spam words, and also can learn what the recipient considers to be spam over time.

If your messages look like spam to these filters, they’ll wind up in a junk folder and the recipient will probably never even see it.

Messages Deleted By Recipients

Even if your email is something a recipient opted-in to receive, and the content is of interest to them, they may simply delete your message without taking any action – perhaps without ever

opening the email at all. For the call-to-action in your message to be effective—telling a friend, buying a product, or accepting an offer, for example—the content has to be engaging and has to prompt the recipient to take the action you desire.

More than ever, ISPs are looking at engagement metrics in addition to complaints and bounces when assessing sender reputation, so the fewer recipients who delete your messages and the more they open or click the better!

Recipients Unsubscribe from Future Messages

At any point, recipients might read a message you have sent and decide they're no longer interested in receiving emails from you. Subscribers unsubscribing from the list will not necessarily harm your reputation as long as they opt-out through a valid unsubscribe link that is included in your email. Unsubscribing should be easy – requiring users to log in, retype their email address or other steps can lead to user frustration and complaints, this process should be as simple as possible.

To make it easy for your recipients to opt-out, consider including an “Instant Unsubscribe” link that requires only a single click in your message. You can do this automatically when you send your messages with RocketMail simply by clicking the “Add a standard Unsubscribe Link” checkbox when you're creating a new campaign.

Continuing to contact someone after they've unsubscribed from your list is illegal and the practice of spammers.

5 | Track the results

Email marketing is an iterative process, as you gradually adjust your audience and your content to get the best results. To do this, you need to track every aspect of your campaign: whether messages are delivered, opened, clicked, forwarded or if they have been acted on.

Tying email marketing initiatives to business outcomes is essential to their success. Doing so tells you what impact you're having on lead generation, online sales, and other core aspects of your business. If you neglect this analysis, not only will you be unable to improve your marketing effectiveness, you will be missing out on important feedback that can impact your reputation and it will be difficult to show the rest of your organization the results of your hard work.

6 | Manage list hygiene

A good email marketing solution will make sure the list you're using is clean. It will remove nonexistent domains and invalid recipients, and will quickly remove recipients who opt out from future emails or complain.

An email marketing platform is not a list-cleaning tool however – ensuring that your list is clean is up to you. Start with a valid, properly qualified list of recipients and an email marketing platform helps to automate some of the ongoing list maintenance as you send emails and build a good sender reputation.

Good list hygiene contributes to your overall reputation, and demonstrates that you're acting according to legitimate email marketing practices—making your message more likely to reach those prospects and customers who want to receive it.

7 | Fine-Tune Content to Maximize Engagement

All of the tracking that you've done means nothing unless you use it to your advantage to optimize your future content. What kind of messages cause an increase in unsubscribes? What offers encourage people to forward the message to their friends? Which prices or colors trigger purchases?

By constantly evolving your marketing efforts using segmentation and campaign analytics, you can maximize the effectiveness of your campaigns. Some emails, even though they're legitimate, simply never get opened. Bad subject lines are often the culprit; marketers need to craft compelling, action-oriented subject lines that convince the recipient to open them.

Online marketing is changing dramatically. A few years ago, marketing was one-way, from vendor to prospect; and websites were relatively static. Today, however, companies need to interact with and engage their audiences. An engaged prospect visits your site frequently, clicks on links in emails, and interacts with a company's brand on social networks. ISPs and email providers are adapting to this change, using the level of recipient engagement as a measure of a sender's reputation. That means if you want a good reputation, you'll need to connect with your market across many different platforms, including email, social media, and the web.

CAN-SPAM Compliance

It is very important to follow the laws that apply to the country (or region) you are sending email to or from. The CAN-SPAM Act of 2003 was introduced in the United States and sets out the minimum

legal regulatory standards that marketers need to adhere to when they send email marketing campaigns. CAN-SPAM applies in a variety of situations:

- (a) If you are sending email to subscribers based in the United States
- (b) If you are sending email to a domain that is hosted in the United States / a US Company (like a hotmail.com, yahoo.com or gmail.com address)

All US based ISPs and web mail providers require compliance with CAN-SPAM. However, compliance is not a guarantee of message delivery as CAN-SPAM specifically allows ISPs and web mail providers to set their own policies governing message delivery. What is important to point out that it only takes **one address** in a contact list to require you adhere to CAN-SPAM or other laws. As a general rule, we recommend that you adhere to the strictest rules of the road to ensure global compliance.

There are two basic kinds of email you might send:

Commercial content

Advertises or promotes a commercial product or service, including content on a website operated for a commercial purpose.

Transactional or Relationship Content

Facilitates an already agreed-upon transaction or updates a customer about an ongoing transaction.

If the primary purpose of the message is commercial, it must comply with the requirements set forth by the CAN-SPAM Act. If your message contains only transactional or relationship content, its primary purpose is transactional or relationship - it must not contain false or misleading header information, but is otherwise exempt from most provisions of CAN-SPAM. That stated it is best practice to not use a deceptive subject line, make sure you tell recipients where you are located and provide recipients with the ability to opt-out from receipt of further messages.

What does this mean? You're allowed to include commercial-based content in transactional emails as long as the transaction remains the email's "primary purpose", with the subject line and message body emphasizing the transaction. This gives you an excellent opportunity to make a good first impression with your customers, but it is a delicate balancing act. If this is not done properly, you risk some hefty fines, generating complaints and affecting your transactional deliverability.

Here's what CAN-SPAM says about commercial mail¹:

1. **Don't use false or misleading header information.** Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
2. **Don't use deceptive subject lines.** The subject line must accurately reflect the content of the message.
3. **Identify the message as an ad.** The law gives you a lot of leeway in how to do this, but you must disclose clearly and conspicuously that your message is an advertisement.
4. **Tell recipients where you're located.** Your message must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.
5. **Tell recipients how to opt out of receiving future email from you.** Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or another easy Internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you. Make sure your spam filter doesn't block these opt-out requests.
6. **Honor opt-out requests promptly.** Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request within 10 business days. You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.
7. **Monitor what others are doing on your behalf.** The law makes clear that even if you hire another company to handle your email marketing, you can't contract away your legal

¹ Taken from <http://business.ftc.gov/documents/bus61-can-spam-act-Compliance-Guide-for-Business>.
Be sure to check the FTC's website for current guidelines.

responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.

The following are links to several anti-spam policies available online. This is not a substitute for legal advice, so in the case of questions, you should consult with an attorney concerning what privacy laws affect you and your organization.

United States: The CAN-SPAM Act: Requirements for Commercial Emailers

<http://business.ftc.gov/documents/bus61-can-spam-act-Compliance-Guide-for-Business>

Canada: Fighting Internet & Wireless Spam Act (Proposed Bill C-28)

<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocID=4547728>

Europe: Privacy & Electronic Communications Directive (2002/58/EC)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF>

Australia: 2003 Spam Act

<http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401898>

For email legislation in other countries, please consult:

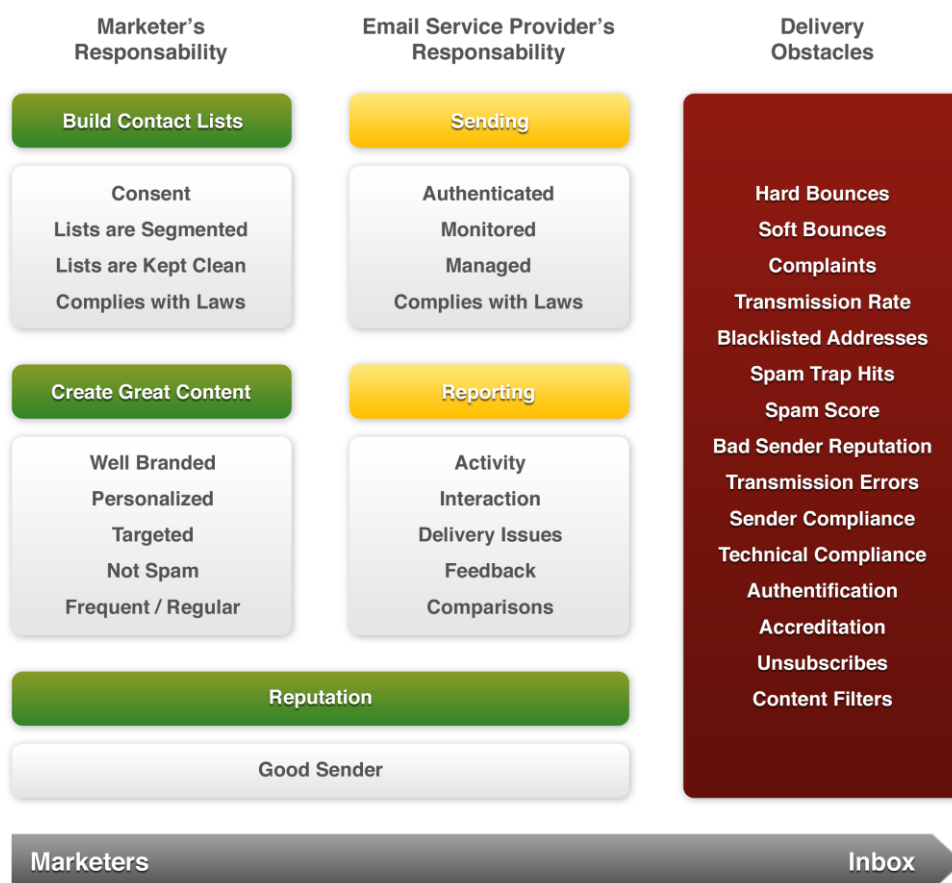
http://en.wikipedia.org/wiki/E-mail_spam_legislation_by_country

The Big Picture

Getting great results out of email marketing starts with getting to the inbox of your subscribers and this is a shared responsibility. As a marketer, you need to start with **the right list** and **compelling content**. These two factors, more than anything else, will drive the success or failure of your marketing efforts. Your email marketing platform needs to do the rest – **monitoring, tracking, reporting and resolving issues** on your behalf so that you can either avoid or overcome the many obstacles that your messages face on their way to each recipient.

Email marketing can be an effective way to engage your customers and drive sales. Do it right, and you'll be connected to your market. Do it wrong, and you may irreparably tarnish your online reputation.

Figure 4: Outlines what parts of the process are the responsibility of clients & their



agencies, which are the responsibility of an Email Service Provider, and what delivery obstacles might get in the way (or need to be overcome) while your email is on its way to your recipient's inbox.

Other Useful Resources:

Messaging Anti-Abuse Working Group (MAAWG)

Sender Best Communications Practices, Version 2.0

<http://www.maawg.org/resources/maawgsendersbcpver2>

Coalition Against Unsolicited Commercial Email (CAUCE)

<http://www.cauce.org>

ESPC

Email Service Provider Coalition

<http://www.espccoalition.org>

Report of the Task Force on Spam

http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00248.html

Network Abuse ClearingHouse – Abuse.net

<http://www.abuse.net>

Authentication and Online Trust Alliance (AOTA)

<http://www.aotalliance.org>

Email Experience Council (ECC)

Part of the Direct Marketing Association (DMA)

<http://www.emailexperience.org>

TRUSTe

<http://www.truste.org>

Spamhaus

How Blocklists Work

http://www.spamhaus.org/whitepapers/dnsbl_function.html

Contact 10fold Solutions

10fold Solutions LLC

1895 Portland Ave, Ste 2

St. Paul, MN 55104

Phone: 651-340-8038

www.10foldSolutions.com

Our Anti-Spam Policy: <http://10foldsolutions.com/anti-spam-policy/>

Our Blog: <http://www.10foldsolutions.com/blog/>

Join Us On Twitter: <http://www.twitter.com/10foldsolutions>

Find Us on Facebook: <http://www.facebook.com/10foldSolutions>

Sign Up Today! <http://www.cakemail.com/signup>

Sales Inquiries: contact@10foldsolutions.com