WHITE PAPER

BEST PRACTICES IN EMAIL DELIVERABILITY

The best email offer in the world will never convert to a sale – if it doesn't first land in a buyer's inbox.

The art of successful direct email marketing depends first and last upon proactive deliverability management – which is simply understanding and complying with the rules that govern business email.

This white paper will help you manage the critical factors that affect the deliverability of your email messages.

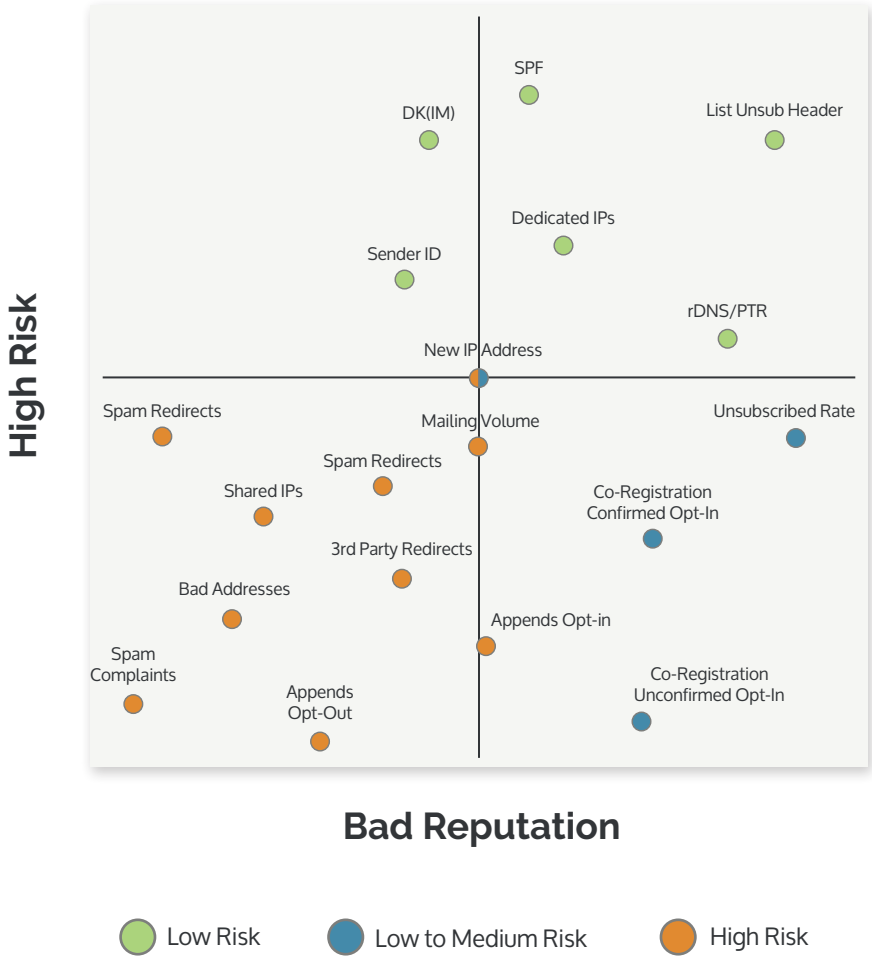
Contents

The Importance of Email Deliverability

"Deliverability" is the measure, usually expressed as a percentage, of how many emails actually make it into the inbox. To create deliverable email campaigns, you must first understand the landscape and the challenges that must be overcome to place a message in an individual's inbox. Because each receiving Internet Service Provider (ISP), business email exchange, and individual account uses significantly different rules, there's quite a bit to learn, and the landscape changes every day.

Because email marketing campaigns are intricate, businesses turn to specialists – such as marketing automation solution providers – to handle much of the mechanics of a campaign. Deliverability is affected by the business processes and reputation of an email service provider, but the most critical deliverability factors rest with you, the sender, regardless of which email marketing solution you use. The factors noted below are all in the marketer's control.

Email Reputation Landmines



Working With Your Service Provider

In the 1990s, as companies began to adopt email as a marketing tactic, email service providers sprang up to help with the technical aspects. Many are still in business today, providing a wide range of services. As digital marketing evolved to encompass techniques complementary to email (e.g. landing pages, forms) or dependent on it (e.g. webinars), new technology – primarily marketing automation – evolved to manage email marketing and integrate these new components, and report on the combined results.

Q1 2016 email volume rose by 25.9% compared to Q1 2015

30% of brands saw statistically significant increases in transaction rates in Q1 2016

– Experian

Benchmarks

Do you know what your current deliverability rates are? Whether you work with an email service provider or a marketing automation service provider, they should be able to provide them to you. Here are the basics to look for:

Email sent

This is how many messages were in the queue before any delivery attempts were made, but after internal suppression has been performed. For Act-On users who subscribe to a number of "active contacts", this is the number counted. This will be a whole number, not a percentage.

Email delivered

This metric describes how many emails were completely transferred to the intended recipient's mailbox provider without generating a "bounce" or other delivery error. There are two levels of delivery:

- If the recipient's email provider rejects the email message, it does not count as delivered. However, if the provider accepts the message, it counts as delivered.
- Once past the provider's filters, the email message must still make it past the recipient's own filters. If the recipient has content-based filters set up that prevent the email from reaching the inbox (e.g., being diverted to the junk folder), it generally will count as delivered.
- This is the metric used to purchase email advertising by CPM or third party list rental. You will see it as a whole number and also as an "Email Delivery Rate" percentage (e.g. "95%").

Email inbox delivered

This metric is an estimation of how many of the Sent emails actually ended up in the inbox. You'll see it as a whole number or as a percentage (e.g. "90%").

Bounces

Bounces are emails that cannot be delivered to the mailbox provider, and are returned to the service provider that sent them. "Hard" bounces are the failed delivery of email due to a permanent reason, such as a non-existent address. "Soft" bounces are the failed delivery of email due to a temporary issue such as a full inbox or an unavailable ISP server.

Email unsubscribe requests

This tallies how many people took an action (such as clicking an "unsubscribe me from this list" link) to unsubscribe from a list.

Working With Your Service Provider (continued)

Complaints
This tallies how many people clicked a spam or junk button link in their email client to report an email as spam or junk.

Other common email metrics, such as Opens and Click-throughs, are also important, as ISPs look at engagement measures to help determine overall how "wanted" an email is.

Shared responsibilities

Your marketing automation service provider will manage certain aspects of your list and email campaign, including bounces, unsubscribes, and feedback. Your service provider will also ensure that your email is RFC compliant (this refers to email standards set by the Internet Engineering Task Force) and may manage aspects of your IP.

The balance of the activities are the domain of the marketer.

MAILING SYSTEMS	BUSINESS POLICIES	REPUTATION	DESIGN & CONTENT	DATA
• Dedicated IP	• Legal Compliance	• Blacklists	• Design & Text Elements	• Frequency
• Shared IP	• Affiliates, Advertisers & Advertising	• Blocklists	• Rendering Issues	• Data Collection & Hygiene
• Authentication	• Data Permission Practices	• Abuse Boards	• W3C Compliant HTML	• Bounce Management
• Volume & Frequency Management		• Spam Complaints	• Link Configuration	• Feedback + Unsubscribe Management
• RFC Compliance		• Collaborative Fliters	• Compliant Headers	
		• User Engagement		
		• Web Site Transparency		

- The green text indicates activities the marketer controls
- The orange text indicates activities the service provider manages
- The black text indicates activities that may be managed by the marketer's company or the service provider

All About Spam, Spam Traps, and Spam Cues

The biggest risk to your deliverability is having your email misidentified as spam. "Spam" is unsolicited commercial email messages. We think of it first in connection with advertising, but spammers also use it to spread malware. Any type of electronic messaging can be a channel, including instant messaging, mobile phones, social networks, and so on, but it's the most disruptive in email.

Spamming persists because advertisers have no operating costs beyond the management of their mailing lists, and it's difficult to hold them accountable. The estimated figure for spam messages (in 2011) is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by internet service providers (ISPs).

As a consequence, ISPs and industry groups doggedly work to develop ways to find and stop spam before it reaches the inbox. It's up to internet marketers to create email and use sending protocols that are squeaky-clean and technically compliant, in order to avoid being identified as spammers and/or having their messages identified as spam.

Spam Traps

Many webmail providers and spam filtering organizations take unused or abandoned email addresses (or B2B domains) and convert them into spam traps. A spam trap is an email address used to lure spam, so the spam can be identified, then added to a blacklist or other blocking mechanism. In theory, a spam trap is an address that has never signed up for any commercial email whatsoever, so any mail it receives is considered spam.

Spam Cues Found in Written Content

Some of the distinctive content differences between wanted and unwanted email are due to the sender's use of written language.

Certain differences are due to senders of unwanted email trying to hide their identity or their content. Many of them are due to the different quality software used to send each sort of email. Mail clients used by individuals, and content composition software used by high-quality service providers, tend to produce well-written code, complying with email and MIME standards, and common practices for email composition.

The software used by spammers, botnets, viruses, and low-quality email service providers tends to write bad code that is not compliant with industry standards. As long as you are using a responsible, legitimate service provider to send mail, and are checking your content to ensure it meets industry standards, these filters should not cause you problems.

Spam Cues Found in HTML Structure

HTML structure evaluation is another aspect of email analysis. Legitimate senders should always use valid and correct HTML. Spammers have long used fake HTML tags in an attempt to avoid filters; now some filters actually look at the tags and compare them with HTML standards. Other spammers put random content in HTML comments as a way to confuse content filters.

The Mechanics of Email Deliverability

How Providers Screen Email

Every internet provider screens and filters incoming emails at some level. You can thank the spammers of the world for flooding the Internet with malware, fraudulent offers, and outright con games, thus making legitimate e-commerce difficult. The goal of the ISP or corporate email server is to reduce or eliminate those nuisance messages from the human user's inbox.

To help your emails make it through the screening process, it is important to understand the deliverability decision factors applied by ISPs.

80% of email delivery problems are directly attributable to a poor sender reputation.

– DMA "Email Deliverability Review"

How Your Sender Reputation Affects Deliverability

ISPs track the reputations of sender organizations. From the point of view of the receiving server, when it comes to IP addresses, past performance is an indication of future results. If an IP address consistently delivers good email, then it is very likely this new email is good, too.

Conversely, if an IP address consistently sends bad email, then it is very likely any new email it sends is bad, too. Many webmail providers and filtering companies offer preferential delivery to senders using IP addresses with good reputations.

ISPs also look at the domains and hostnames mentioned in an email. Just for starters, you've got an unsubscribe link, your company's link, and a link to view the email in the browser. You could also have links to landing pages, registration forms, affiliates, and tracking links. These are evaluated based on the reputation of the domain, and sometimes the IP address the domain or hostname points to.

Domains and URLs have their own reputations separate from the reputation of the sending IP address. Unlike a standard blacklist, which looks at the IP address sending the actual email, a domain blacklist (DBL) or Uniform Resource Identifier (URI) blacklist looks at the individual domains within the email. Domain-based blacklists provide an extra layer of protection for companies using spam-blocking appliances.

The key factors in your reputation are:

- Authentication
- Bounce management
- List cleanliness
- User engagement (recipient feedback)

The Mechanics of Email Deliverability (continued)

Authentication

Email authentication is a technical standard that tells receiving email servers that an email actually does come from the place it says it comes from. Senders use it to establish and underscore their authenticity, which aids in delivery. It's a necessity when sending commercial email.

Most organizations using a commercial service provider generally use the service provider's authentication.

In other situations, an organization's IT department will set up authentication. For solid technical data about authentication, see the Internet Engineering Task Force, www.ietf.org.

Here's a quick overview of the most common authentication methods:

- Sender Policy Framework (SPF) allows administrators to specify which hosts are allowed to send email from a given domain by creating a specific record in the Domain Name System (DNS).
- Sender ID is based on SPF, but it has additions, such as verifying the header addresses that indicate the sending party.
- DomainKeys is an email authentication system that goes a step further; it's designed to verify the DNS domain of an email sender and the message integrity.
- DomainKeys Identified Mail (DKIM), built on DomainKeys, associates a domain name to an email message, thereby allowing a person, role, or organization to claim some responsibility for the message. The association is set up by means of a digital signature that can be validated by recipients.

Bounce management

- Soft bounces are usually due to a temporary factor, such as an overloaded receiving server. It's okay to re-send to them, although at some point (say three soft bounces) it's good to put them into a suppression list.
- Hard bounces indicate an address is no longer good. Don't just suppress them; move them out of marketing lists regularly.

Blacklists and Block Lists

Webmail providers build internal or purchase externally produced blacklists – also known as Block Lists. These are lists of IP addresses that will be blocked to prevent spam, viruses, or phishing emails from reaching the end user. Some blacklists cover domains commonly found in spam. Some list domains or IP addresses from specific countries.

The Mechanics of Email Deliverability (continued)

Engagement

Internet service providers track how engaged subscribers are with an email and its sender, and the nature of the engagement.

Positive actions tracked may include opening a message, adding an address to the contact list, clicking through links, clicking to enable images, and scrolling through the message.

Negative actions may include reporting the email as spam, deleting it, moving it to the junk folder, or ignoring it.

Engagement ratings are another compelling reason to use only opt-in email marketing lists. Opt-in maximizes the likelihood of engagement, because in theory there is a relationship already established with the receiver.

Tips for managing engagement:

1. **Send content that your subscribers expect and appreciate**
   Segmenting your lists and mailing high quality content in specific areas of known interest is always a good strategy.
2. **Set subscribers' expectations**
   Give people who opt in to your subscriptions lists choices of how often they'll receive emails from you (e.g., once daily, a weekly round-up, as items become available or go on sale). If you send infrequently, make that clear. Ask them to whitelist you as they opt in.
3. **Deploy a good onboarding program**
   Let people know when they sign up that they'll receive a welcome email so they'll be expecting it. Jump-start a deeper engagement by telling them who it will be from (a person, not a role or an anonymous address), and be clear about when and how often you'll be mailing them. This will (among other things) validate that your system has noted their preferences accurately. Suggest that they whitelist you if they haven't already.
4. **Keep your lists clean**
   Begin with your registration forms. If you have the option to block spammy, personal, or role-based addresses, do so.

   As your lists age, weed out bounces and unengaged subscribers. Your timing for this depends on your business and your typical sales cycle for this type of customer.

Tip:

One best practice is to purge disengaged addresses before too many accumulate. Determining how long a contact should stay on your list without engagement, and defining a process to manage inactive contacts, requires an understanding of your particular market and demographics.

How Email Sending Schedules Affect Deliverability

When you've created and tested your email message content, and you're confident it should not trip any spam or other filters, then it's time to actually schedule and send your email campaign. As with all other aspects of email, there are factors you can control to enhance deliverability.

Cadence and frequency

The optimal frequency of an email campaign is directly related to the buying cycle. The shorter the cycle, the more acceptable a greater frequency will be to your prospect. If you email too frequently, some recipients will grow irritated and unsubscribe or mark your emails as spam. The former loses you a prospect but does not harm your sending reputation. Getting your email marked as spam, of course, does hurt your sending reputation.

What day and time to send

Recommendations about which days and times to send abound. Opinions range from general rules of thumb like "don't send first thing in the morning" to specific times, such as "send on Tuesdays at 7 a.m. Eastern time."

None of these matter. Your company, your position in the market, and your prospective buyers create a unique combination of factors calling for a tailor-made and tested solution.

Test, test, test

You'll need to test your way to success, and keep testing as external factors change. Test timing separately from testing messaging. After testing, set your own benchmarks and work to your plan consistently.

Email and Content Filters

Email Filtering

Email delivery is a complex process with many stakeholders influencing the outcome. Email filters interact with an email during different stages of the process to determine the answers to the following questions:

1. Should this email be accepted?
2. Should this email be delivered to the inbox or the junk folder?
3. How should this email be displayed?
4. Does the email contain any malware or other intrusive data?

The first stage of filtering begins when the sending webmail server first contacts the receiving webmail server. The receiving server must decide whether to accept the email or not.

At this point, the only thing the receiving server knows about the email is the IP address of the server sending the email. The first thing the receiving server looks at is the reputation of that address, including the authenticating information that indicates that the email really did come from that address and sender.

Email that passes all the evaluation checks gets accepted into the receiving email server and is passed on to the next filtering stage. Email that fails all evaluation checks is rejected. Email that falls into a gray area can be tagged; accepted, deleted, and passed onto further filters; or deferred for later.

Content Filters

Content filters look at a range of things, from the simple to the complex: word use, misspellings, the ratio of text to images, font colors, the subject line and actual text in the message, and much more, including the hidden structure of an email.

Some filters take a "fingerprint" of the email. They can compare the fingerprint with a database of known spam and known good email and determine how like spam the email is. Some tests look for distinctive features from particular pieces of software. For instance, there was a piece of spamware that used a fake time zone value in its email headers. Email with that value was always spam.

Content filters look at domains, links, and images

Many email content filters look at domains, URLs, links, and images in an email, including:

- Has this domain ever been seen in email before?
- Has email with this domain generated complaints?
- Does the plain text part of the link match the domain listed in the <a href> tag?
- Has this domain been listed on any domain-based blacklists?
- Have we blocked this domain in the past?

Best Practices for List Management

Few things affect your email deliverability more than maintaining clean and accurate email lists of engaged subscribers. Even the best lists need constant maintenance. Between the constant turnover of email addresses (something like 30% of subscribers change email addresses annually), loss of interest, and other factors, your email list starts getting stale just as soon as you create it.

The staler a list gets, the fewer opens, clickthroughs, and purchases it generates. This threatens your engagement and potentially your reputation scores as a sender. Follow good list management protocols to keep your engagement high and your reputation for integrity intact.

Dun & Bradstreet studies found that data decays at the rate of 1% to 3% per month, and that poor data quality costs the U.S. economy six hundred billion dollars annually.

Best Practices

- Send only to people who want and expect your email; contacts who opt in are your best prospects
- Confirm or double-confirm subscribers who opt in, when possible
- Encourage recipients to add you to their address books, and make it easy to do so
- Have a clear privacy policy for subscribers
- Grow lists organically; never buy them
- Develop online forms that encourage people to indicate their interests; use this data to create targeted subscription lists
- Make it easy and obvious for contacts to opt out
- Honor "unsubscribe" requests immediately – it's the law
- Determine an optimal mailing time and frequency, and stick to it, for consistency
- Clean your lists regularly

Keep your lists clean and current through purging and re-engaging

Purging your lists can be a difficult exercise, because no one wants to lose potential customers. Yet your online reputation depends on maintaining a clean, healthy email list.

How you implement purging your email list is just as important as deciding what to purge. The two best options for purging are:

1. Simply remove any addresses that meet purging criteria (usually time and lack of activity) from all future mailings
2. Send a re-engagement email asking users to take an action to stay on the list

You should plan to purge any address displaying no activity for 12 months. But the timeframe that works for you depends on the buying cycle, engagement, and conversion for your products or services.

Too often companies don't think about purging data until significant email delivery problems have surfaced. If you wait until your email is blacklisted or delivered to the junk folder, you risk having to make much more aggressive purging decisions than marketers who proactively manage their data.

Best Practices for List Management (continued)

Re-engagement

Sending a re-engagement message offers a chance to win back the recipient. A re-engagement message usually alerts a recipient that their subscription is expiring due to lack of activity, and entices the user to opt in again to continue receiving the email.

Re-engagement messages provide the benefit of shedding abandoned accounts or spam traps from your list. Your list will lose some numbers, but usually the people lost were unengaged, poor prospects anyway.

For very valuable lists, marketers may use a series of emails enticing the recipient to come back. This can have a better response rate than a single email. If a subscriber doesn't interact with the re-engagement email, then it's time to remove their address from future sends.

The 1-10-100 rule

According to SiriusDecisions: "It takes $1 to verify a record as it's entered, $10 to cleanse and de-dupe it, and $100 if nothing is done, as the ramifications of the mistakes are felt over and over again."

Best practices for list cleaning and maintenance

- Clean your lists on a regular basis. We recommend that you perform a cleansing each time you add to your house file, in addition to a quarterly cleansing (at a minimum)
- Remove distribution, role-based, or administrative addresses such as "sales@abc.com" or "info@abc.com"
- Monitor feedback loops so you can identify and immediately remove people who complain
- Understand the engagement cycles of your sales process
- Identify the point where recipient engagement drops; segment disengaged subscribers by useful criteria, such as whether they ever made a purchase
- Re-engage inactive contacts with messaging and offers targeted to their specific segment
- Purge inactive, unengaged contacts when necessary

Email Content Tips for Deliverability

By investing in high-quality content, you will give your campaigns the best possible chances for success:

- Present your brand clearly and deliver content that supports your brand strategy
- Make sure the offer has enough value to make your customers glad they got the email
- Don't neglect proofreading – a spell checker is not enough!
- Determine an optimal mailing time and frequency, and stick to it

Make sure that your email renders correctly in HTML and that all graphics are high quality. Make sure your technical team takes the time to fill in all HTML metadata, such as alt tags on images. A service such as Litmus can help you review how your email message will render in various email clients and devices.

Creating Great Content

Great content in an email marketing campaign is easy to describe, but hard to create. Truly excellent content aligns with your company's brand strategy, presents a clearly actionable opportunity to the reader, enhances your deliverability reputation, and delights your customer.

- Write a subject line that creates an expectation that the body copy will fulfill. Make it short; most email programs will display only 60 or fewer characters (including spaces)
- Short, compelling emails are more deliverable (and tend to get better results)
- Make links obvious, with link title, color, and placement
- Make sure all links point to valid website locations
- Create your message so it displays well in the preview pane; 600 pixels is a good maximum width. Keep your call-to-action above the fold
- A giant image is a spam characteristic. Use images sparingly, don't put important text into images, and have a high text-to-image ratio
- Use alt text on images (so they don't show up as boxes with little red Xs)
- Minimize or eliminate Flash and JavaScript
- Add a line suggesting people whitelist your sending address
- Offer a clear, direct method of contacting you
- Don't use "Dear" as a salutation
- Don't use "click here" or "click below" to offer links to people. Use link title, color, and placement to signify links
- The phrase "for only" followed by a dollar sign is a sign of spam. Mention pricing using other terms, such as "reduced to" or "Member price" or a phrase you've used before that works, or simply state it
- Toll-free phone numbers may get your email tagged as spam if there are additional suspicious signs
- Using ALL CAPS is a spam characteristic
- Use exclamation points sparingly, and don't use several in a row
- If you're mailing to an opt-in list, add a line at the top reminding people that they opted in

Global Email Compliance Obligations

Disclaimer:
Email is governed by laws which vary from country to country. The United States' CAN-SPAM and other legislation are legal issues which affect your email marketing processes and protocols, but do not, by themselves, affect the deliverability of your email.

This information is provided as a general guide only, and is not to be considered or perceived as legal advice. Every organization will be affected differently, based on the destination country of the email you are sending.

We encourage you to seek legal counsel for answers to any questions.

U.S. Laws

In the U.S., the law covering email marketing is The CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing) Act. This law says that all email must meet a number of criteria:

- The sender must provide accurate routing information about the emails.
- The advertising emails must be clearly labeled as advertisements.
- Recipients must be allowed to opt out of emails. Opt-out mechanisms can be either electronic or postal (a P.O. box is allowed). You are not allowed to require more than the recipient's email address and their choice to opt out. This means that companies may not require passwords or other information in order to process the opt-out.
- All emails must contain the physical address of the sender (a P.O. box is acceptable).
- Note that CAN-SPAM does not require that senders have permission to send mail; permission is not a requirement under U.S. law, but is certainly a best practice. In many other countries however, senders must have permission to send marketing and commercial email.
- Sending mail without permission to recipients in jurisdictions with opt-in rules such as Europe or Canada may open up the sender to legal liability. Some senders have attempted to bypass this by segmenting lists by country, but segmentation assumes that the companies selling lists are correctly compiling the data. Obtaining recipient permission before sending protects the sender from inadvertently violating opt-in laws.
- CAN-SPAM applies to all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites.
- Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000 per recipient.

Outside the United States

Privacy laws in the E.U. and elsewhere are more stringent than in the U.S. Please see Appendix E, International Email Privacy & Consent Guide, for more information.

The Send Checklist

Before you hit the Send button, review these items:

Preview your emails to see how recipients will view them in various inbox clients. Make sure your messaging is clear even when images are disabled.

Have you created a plain text version? Make sure the content is very similar to the HTML version, to avoid resembling spam.

Have you cleaned your lists recently? If a list has a lot of suppressions, it will take significantly more time to send. The longer the list, the longer the delay.

When scheduling multiple messages, schedule the smaller sends first; they will take less time to process and launch.

If a given message is time sensitive, give it extra time and schedule it to start earlier than you normally would. For example, if you normally schedule the launch for 10 a.m., schedule for 9 a.m. instead.

Spammers send frequently, and they send to big lists. If your patterns are the same, make sure your IP address, content, and list are squeaky clean.

Track Your Response Rates

Track your email response rates, including deliveries, clicks, responses, non-responders, bounces, and actions taken on any external links that are in an email. Reporting is the key to understanding and improving your campaign performance, and it has a role to play in delivery assurance as well.

It's important to know what your average delivery, bounce, and engagement rates are, so you'll see anomalies clearly and quickly. The rates below are industry averages; bear in mind that numbers vary widely from industry to industry, and that various service providers and marketers may calculate them using different formulas. Develop and use your own benchmarks. If your results suddenly worsen, investigate.

Here are a few broad guidelines:

- B2B email newsletter click-through rates generally range from 5%–15%. Low open and click-through rates may indicate that your content isn't interesting, or you aren't giving people obvious links or good reasons to click them.
- B2C email marketing promotional campaign click-through rates generally range from about 2%–to 12%. Low open and clickthrough rates may indicate that your list or offer isn't good.
- The more targeted and personalized your email is, the higher your rates will be; in B2B, a click-through rate of 10%–20% is good.
- Trigger emails (those sent as an automatic response to an action a prospect takes, such as a website visit) achieve 76.7% higher open rates and 226.9% higher click rates compared to Business As Usual (BAU) messages, according to Q4 2015 data from Epsilon.
- A "spam complaint" occurs when a recipient marks your email as spam, not when a webmail provider filter tags your email as spam. Note that unsubscribes do not hurt deliverability, but spam complaints and hard bounces do.
- If suddenly you have a spike in your bounce rates, look first to email content and structure. Your marketing automation service provider may be able to provide feedback about probable or actual causes from webmail providers, and should share that information with you.

Consistently low rates suggest that your email is uninteresting or your list is bad. Either will lead to higher "delete" rates, which will affect your reputation and delivery.

Appendix A: What Spammers Do

Every legitimate email marketer wants to be sure not to be mistaken for spam. Table A offers some quick dos and don'ts from SpamAssassin and the Apache Software Federation to help you avoid a spam label:

Are You a Legitimate Mailer?	...Or Do You Look LIke a Spammer?
Use email composition and mailing tools that work correctly. Well-constructed emails (technically correct) can be readily identified as not-spam.	Emails with missing mime sections, invalid or missing message-ids, invalid or missing date headers, subject or other headers with unescaped Unicode (and so on), are frequently spam.
Don't include a disclaimer that your email isn't spam. Don't claim compliance with some legal criteria, especially one which is not actually law in your country.	Only spam needs to claim compliance – non-spam is supposed to already be in compliance
Use normal conversational language. Don't use excessive spacing and/or capitalization in your subject line.	Spammers use "cute" spellings, S.P.A.C.E out their words, and put str@nge |etters 0r characters into their emails.
Do not use invisible text within emails. Make sure your text colors and sizes are distinct enough and large enough to read.	Invisible text is often identified as a sign of spam.
Do not use invisible web bugs to track your emails. If you must track your emails and whether they're read, use visible graphics.	Spammers try to hide malware in invisible elements.
Don't use "bulk-mailing" tools used by spammers or advertised through spam.	If a bulk mailer's product's feature list includes "stealth sending" or similar terms, all mail sent by that program will be treated as spam elements.
Be careful where you advertise, and be careful which advertisements you carry.	Spammers advertise with companies that send out spam, and their domains are flagged as being related to spam.
Be visible and public in your domain and hosting registrations.	Spammers use bogus entries in domain registrations, or "private" or "hidden" annotations.
Make sure you have active and monitored abuse and postmaster email addresses. Register them with abuse.net.	Spammers try to hide from unpleasant public feedback.

Appendix B:
Best Practices for Retention Email

Retention email's primary focus is to obtain, nurture, and retain a customer relationship once you have established the initial permission to make contact.

For example, let's say that Mary buys something from YourStore and provides her email address and permission to contact her after her initial transaction. At this point, Mary is 100% opted in to your program – this is good. What you do next will establish your ability to communicate with Mary and ultimately drive ROI with strategies and offers based on her preferences and expectations.

To begin with: Now that you have her attention, it's imperative that you get her engaged with your program almost immediately to ensure continuity and deliverability.

Begin the on-boarding experience

- Send a welcome message: thank her for signing up, etc.
- Set expectations on frequency and content that she will receive
- Provide instructions on how to add your "From" address to her safe sender list
- Explain the message outreach. "This is message 1 of 5," for example. Explain what's coming in future communications
- Allow her to reset her preferences at any time; put her in control of her experience
- Personalize your messages; remember, Mary probably doesn't want to receive emails with information that's not important to her

As your customer becomes more engaged, this engagement in turn will enhance your deliverability, reputation, and ROI.

Best practices for retention email

- Deploy a great onboarding program; make it engaging
- Keep gathering data on your customers; don't take their preferences for granted. Things change!
- Send thank-yous for purchases and touch base periodically; check in with your clients
- Send invitations and reminders of events based on past behavior or purchase history
- Send announcements of new products, promotions, or services based on past purchases
- Encourage social sharing for your brand – this helps build client loyalty
- Segmentation works; one size, message, data point, or product definitely does not fit all
- If possible, use an IP address for transactional and acquisition emails that is different than the one you use for retention
- Be consistent in your relationships with your clients

Appendix C:
Best Practices for Acquisition Email

Acquisition email's most common goal is to convert potential leads into sales- and retention-based customers; the barriers to success are more complex than the retention-based email activities.

One of the key factors driving acquisition success is data (email addresses in this case) and the way it's collected and permissioned.

Many organizations supply (rent or sell) email addresses that have a level of permission (presumably opted in) that will allow you to send them communications. The usual strategy is to use this data in the early stages of list growth, to build your house file to a minimum size. **This is not a best practice**; it is, in fact, rather risky. Most such lists will contain spam traps or other outdated/undesirable data that can do serious harm to your sending reputation.

So how does it work?

A scenario: A marketer acquires a list of addresses through a third party and emails an offer to the list, hoping that some percentage of those recipients will be interested in what the marketer's company is selling.

Here's how addresses get on that list: Suppose you bought a product or signed up for a webinar, and didn't read the fine print … in which the vendor stated that unless you opted out of something, your email address would be shared with third parties. Your email address then went into a list comprised of other addresses gathered the same way. The third parties rent or sell that same list to lots of organizations that will use it to conduct acquisition email campaigns.

As a worst-case scenario, let's say your company buys a list and sends an email to an individual named "Tom." You know nothing about Tom. His name got on this list because he once bought a product or attended a webinar, and he forgot to opt out of having his data shared. And Tom knows nothing about you. So if you send him an email about a product or service, it likely has NO relevance to him whatsoever.

Tom's a busy guy, so the irrelevant email irritates him and he hits the "Mark This as Spam" button. So do a lot of the other people on that list. This results in a high complaint number, which in turn results in negative deliverability and reputation for your email sending program. Not good.

As you can see from the example, the risks to acquisition email campaigns are high. Especially as you are potentially relying on third parties to supply you with the data (and its accompanying permissions) to initiate the outreach.

Appendix C:
Best Practices for Acquisition Email (continued)

However, with a little change in plans and program management, you can use the acquisition channel to your benefit. Here are tips for success:

Best practices in acquisition email

- If your goal is to convert data for list-building purposes, then adopt some of the tenets of retention-based marketing, such as welcome programs, onboarding, etc.
- Deal only with reputable data organizations. NEVER acquire data from the web or from sources you don't trust. If the cost of the list and the volume sound too good to be true, then it probably is
- Delete non-responders immediately. Names that don't respond are not interested in what you have to say, period; if you don't remove them, your deliverability will suffer. Do not procrastinate this task
- Mail only to people who have opted in and have had proven engagement with the data provider. This information may be hard to get; we recommend that you ask for opt-in logs
- Mail based on some known factor, such as interest in a specific product or other relevant factor
- Watch your deliverability like a hawk; high bounce rates are an indication that a list is old and non-engaged
- Make it easy for the lead to unsubscribe. It's better for your reputation to have ten people unsubscribe than to have one mark a message as spam
- Shift your focus from a quick sale (one and done) to nurturing the lead. This will provide longevity in the contact and ultimately better ROI
- If possible, use an IP address for transactional and acquisition emails that is different than the one you use for retention
- Be patient. List building (organic or by acquisition efforts) is a marathon and not a sprint

Acquisition email is hard to do. There are many pitfalls and barriers in place to trip marketers up and limit campaign progress. In the context of the entire email ecosystem, acquisition email falls on the low end of the ladder.

Take small steps as you enter the acquisition channel... take it slow. Know your audience, your vendors, your data, and most of all – your deliverability.

Appendix D:
Best Practices for Transactional Email

Messages that have NO commercial content at all are considered transactional email messages and don't have to comply with CAN-SPAM or other laws pertaining to commercial electronic messages (CEM). (This is generally true outside the US, but consult with your legal consul to be certain.). Order confirmations, promotional messages, and informational newsletters are examples of transactional communication. Where marketers may get into hot water is when they use the transactional message to cross-sell or upsell their commercial products in the same message.

Let's take a look.

The Primary Purpose rule

When you use transactional messaging to promote your commercial products under CAN-SPAM, the Primary Purpose rule comes into effect. This is where the gray area of transactional messaging kicks in, and it can easily be misunderstood.

Under the Primary Purpose rule, if the recipient perceives that the "primary purpose" of the message they received is commercial in nature, then the message MUST be CAN-SPAM compliant, without exception. That means: No matter how certain the marketer is that the message's primary purpose is transactional...it is the recipient's perception that determines whether the message is commercial. This is not a negotiable issue.

There are a few other interpretations of the Primary Purpose rule under CAN-SPAM, but it's better to comply than not.

So, what factors would drive a recipient to think that a message is "commercial" in nature?

- Leading with the offer BEFORE the transactional information
- Placement of commercial images within the body of the message
- Too much "offer real estate" in the message, dominating the theme

Best practices in transactional email

- During your onboarding or preference center user experience, ask your client if they would like to receive cross-promotional messaging within their transactional messages. If they say no, honor their preferences
- Ask clients to add your "From" address to their safe senders list or address book to ensure deliverability continuity
- Place any offer "below the fold" of the email
- Keep the offer's real estate within the message to a third of the message itself
- Ensure that all transactional messaging that contain offers are CAN-SPAM compliant
- If possible, use an IP address for transactional and acquisition emails that is different than the one you use for retention
- Manage your deliverability; transactional messages generally are better performers for engagement because of the intent of the message and the expectation that it's going to arrive

Appendix E:
International Email Privacy & Consent Guide

	EXPRESS OPT-IN CONSENT REQUIRED?	OPT-IN TIME LIMIT?	OPT-OUT NOTICE REQUIRED?	TIME TO LIMIT PROCESS OPT-OUT?	PHYSICAL ADDRESS REQUIRED?
North America					
United States	No	Forever until withdrawn	Yes	10 business days	Yes; corporate postal address
Canada	Yes	Forever until withdrawn	Yes	10 business days	Yes
Europe					
Belgium	Yes	Forever until withdrawn	Yes	Within reasonable time	Yes
Czech Republic	Yes, other than current customers	Forever until withdrawn	Yes	Immediately	No, but valid email address required
Denmark	Yes	Forever until withdrawn	Yes	No time limit	No
France	Yes	Forever until withdrawn	Yes	Within reasonable time	No
Germany	Yes	Forever until withdrawn	Yes	Two weeks	No
Hungary	Yes	Not specified	Yes	Immediately	No
Ireland	Yes	Forever until withdrawn	Yes	Not specified	Yes and sender identity request
Italy	Yes	Forever until withdrawn	Yes	Within reasonable time	No, but contact data required
Netherlands	Yes	Forever until withdrawn	Yes	1 month	Yes
Norway	Yes, other than current customers	Forever until withdrawn	Yes	No time limit	No
Poland	Yes	Forever until withdrawn	Yes	Not specified	Yes
Sweden	Opt-in required for B2C email	Forever until withdrawn	Yes	As soon as possible	Yes, but not necessarily from within the country
Switzerland	Yes	Forever until withdrawn	Yes	Not specified	No, but sender identity required
United Kingdom	Yes	Forever until withdrawn, unless specified in the opt-in notice	Yes	Not specified	No, but sender identity required
Asia					
China	Yes	Forever until withdrawn	Yes	Not specified	No
Hong Kong	No	N/A	Yes	10 business days	Yes; sender's corporate address, name, phone number and email address required
Israel	Yes, unless the recipient: gives their contact details during a purchase; chooses not to opt out; or made a purchase similar to what the email concerns	Forever until withdrawn	Yes	Not specified	Yes; sender's corporate address, and contact details required
Japan	No, but if consent isn't obtained, the sender must follow certain regulations	N/A	Yes, in emails sent without permission or a business relationship between sender and recipient	Immediately	No
Singapore	No	N/A	Yes, if the message is unsolicited, bulk, commercial, and electronic	10 business days	Yes
South America					
Argentina	No	N/A	Yes	5 business days	Yes
Africa					
South Africa	No	N/A	Yes	Not specified	Not specified
Oceania					
Australia	Yes, other than current customers	Forever until withdrawn	Yes	5 business days	No, but contact data required
New Zealand	Yes, other than current customers	Forever until withdrawn	Yes	5 business days	No, but contact data required

Acclaim for Act-On

FROST & SULLIVAN
2014 BEST PRACTICES AWARD

Inc. 500 2013, 2014, & 2015 FASTEST GROWING COMPANIES

Forbes 2013
AMERICA'S MOST PROMISING COMPANIES

Deloitte.
Technology Fast500

LEADER in Forrester Research, Inc. report, The
FORRESTER WAVE
Lead-To-Revenue Management Platform Vendors, Q1 2014

See all of Act-On's awards & accolades...

About Act-On Software

Act-On Software is a marketing automation company delivering innovation that empowers marketers to do the best work of their careers. Act-On is the only integrated workspace to address the needs of the customer experience, from brand awareness and demand generation, to retention and loyalty. With Act-On, marketers can drive better business outcomes and see higher customer lifetime value. The Act-On platform provides marketers with power they can actually use, without the need for a dedicated IT resource.

Connect with us to learn more

www.act-on.com