ORACLE MARKETING CLOUD

Email Deliverability

GUIDE FOR MODERN MARKETERS – 2016

ORACLE

Delivering the Goods

Why Email Deliverability Is More Important Than Ever

"Are your customers engaged?"

That's the question that all email marketers should be asking ourselves as we're evaluating the success of our programs. The engagement buzzword of the past few years has been replaced with the reality of dealing with these engagement metrics as a major driver of deliverability success. Sophisticated email receivers like Gmail have taken engagement-based actions to new levels.

The side effects of these changes are far reaching today. Not all marketers have adapted to this new reality. The old school way of sending more and more email was a mentality created by the management food chain that email marketing was easy. Executives saw this as an affordable channel that seemed to have unlimited scalability. If you sent out 100 email messages today and generated $10 in revenue, it stood to reason that if you sent 200 messages out tomorrow you would generate $20. Batch and blast was off and running.

In today's world, where an estimated 216.6 million Americans are email users, which represents nearly 89 percent of total internet users, it's not enough to simply hit the inbox to run a successful email program. Your recipients have to interact with your messages—they have to open and click around. Today's reality demands that you center your marketing around the customer by orchestrating messages that are relevant to each individual's preferences and behavior.

This means sending less email and paying more attention to the data you've collected about your customers. If you aren't paying attention to segmentation, dynamic content, and engagement, you will find that a majority of your messages end up in a bulk or spam folder.

In addition to the normal concerns associated with deliverability, there has been an explosion in the number of senders who have gone global. Understanding the differences in what is necessary from country to country is now an integral part of overall success.

It should be no surprise that getting your messages to the inbox is absolutely critical these days, especially if you're using email as the way to kick off an orchestrated marketing program.

In this guide, we cover the latest intelligence related to email deliverability best practices, the changing ISP landscape, international regulations, and deliverability strategy. There's also a handy global list at the end.

We hope you enjoy the read and use it for future reference.

—The Oracle Marketing Cloud Deliverability Team

> "Are your customers engaged?"

2016 EDITION

- New information on ISPs
- Updated email address acquisition best practices
- New international sending guidelines
- Program optimization from a strategic perspective

Email Acquisition Best Practices

Good email deliverability starts at the beginning when you acquire an email address. And asking for permission and setting expectations are two basics when it comes to email acquisition.

The most significant deliverability problems are the result of problems with the email signup process. While a particularly acute problem for retailers collecting addresses in store, the signup process can cause trouble for any business collecting addresses. New signups can introduce major problems into your otherwise well-tended email list.

Like arranging a first date, you first have to ask permission to get his or her phone number. It's no different here. You need to ask permission to acquire someone's email address.

Like setting expectations for that first date, you want to do the same thing with your email database. You want to set expectations about what they will be receiving from you going forward.

> “You need to ask permission”

Tread Carefully with New Signups

Experts say sending email to new signups always carries an elevated risk of triggering spam filters, due to the unproven nature of the new email address. For this reason, it's very important to stay current with your welcome campaigns. The risk of triggering spam filters is compounded if you ever find that you have a backlog of new email signups.

If you find yourself with a backlog of new signups, don't email to them all at once. This can trigger blocking and filtering. Spread out your sending to these new addresses over days or weeks, keeping a low volume of welcome messages each day relative to your regular email volume. This will help minimize any negative impact to your sender reputation and delivery rates.

The following poor email acquisition practices increase the risk of triggering ISP filtering or blocking:

- High hard bounce (invalid) rates
- High spam complaint rates
- Low response and subscriber engagement rates
- Spam trap hits
- Volume spikes
- Unaccepted flavors of opt-in

Oracle recognizes the following subscriber acquisition methods as consent:

Method	Description	Notes
Closed-loop Confirmation (also Double Opt-in)	Unchecked box with follow-up email that requires further action to confirm	The gold standard of consent
Opt-in	Unchecked box (with or without follow-up email)	Welcome Email recommended
Checked-Box Opt-in	Pre-checked box in conjunction with a prior business relationship ONLY (with or without follow-up email)	Requires overt messaging & submit button
Offline Opt-in	Paper form, telephone conversation, in-person conversation	Requires overt messaging & script documentation
Opt-in Confirm	Email invitation to opt-in sent to customers with a previous transactional business relationship	Opt-in invitation may not contain promotional material

Double Opt-in and Opt-in Confirm are the strongest methods of acquisition and should be utilized when acquiring addresses through riskier channels such as POS collection. Those subscribers that enter your list through Double Opt-in/Opt-in Confirm are showing that they truly want to hear from you and will likely show higher engagement levels with future campaigns. This method also helps prevent bad addresses from entering your list.

Opt-in and Checked-Box Opt-in are the two most common methods marketers employ today. Although a follow up email or welcome email is not required it is highly recommended.

Offline Opt-in and Opt-in Confirm are less reliable methods and can potentially degrade the quality of your list. With these methods, you run the risk of collecting faulty email addresses and/or generating high spam complaints.

Stay Away from Appends, Rentals, and Purchased Lists

These tactics erode brands and create major deliverability issues. The address segments are characterized by a lack of response—very low open and low click rates. And because these users had never expected to receive email from the sender, the lists can generate many spam trap hits, higher bounces, unsubscribes and complaints. That puts the sender's deliverability reputation at risk and requires a great deal of effort to restore.

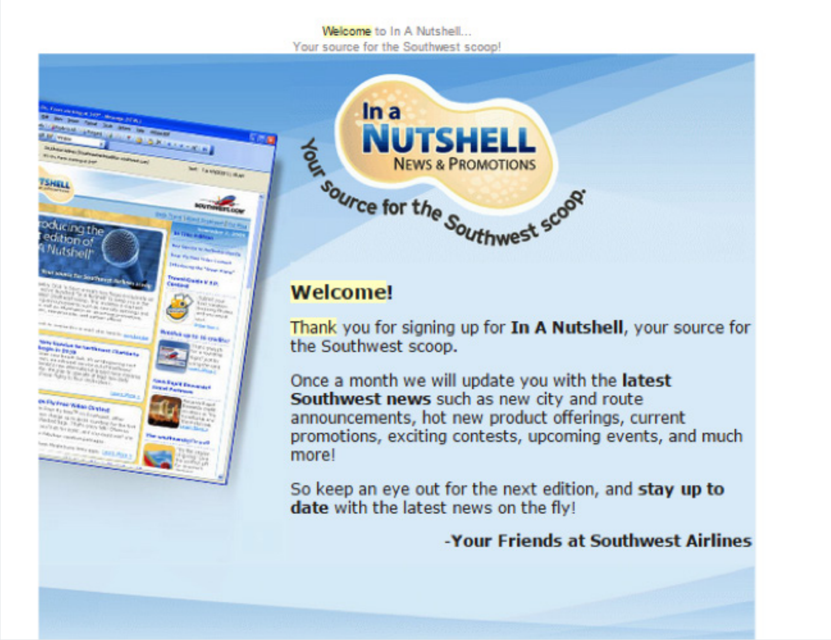
Due to the highly unreliable nature of addresses being collected, the possibility that the sender's IP could become blacklisted greatly increases. This can be especially damaging at widely used blacklists such as Spamhaus. Once an IP is blacklisted, then any email messages from that IP will be blocked by ISPs referencing that blacklist.

Create a Strong Welcome Program

When a subscriber is first added to your list, it is a good idea to send them a series of emails welcoming them to your program. With these emails, you should clearly communicate your opt-in/permission policy and set expectations for what is to come in future emails. You should also use this opportunity to let them know how often they can expect to receive your emails and how to opt-down or change their preferences if necessary. A simple welcome campaign can go a long way in establishing a good relationship with new subscribers.

> “A simple welcome campaign can go a long way”

Welcome Example:



Welcome to In A Nutshell...
Your source for the Southwest scoop!

Welcome!

Thank you for signing up for **In A Nutshell**, your source for the Southwest scoop.

Once a month we will update you with the **latest Southwest news** such as new city and route announcements, hot new product offerings, current promotions, exciting contests, upcoming events, and much more!

So keep an eye out for the next edition, and **stay up to date** with the latest news on the fly!

-Your Friends at Southwest Airlines

Why Long Term Inactive Addresses Still Matter

Now it's time for us to bust a myth dealing with long-term inactive email addresses. You may be under the impression that these types of addresses are not relevant when it comes to acquisition.

The truth is you have to be concerned because people will create a new account and sign up with an email address that they long ago abandoned. Additionally, they may make a typo and the resulting email address happens to match a spam trap email address. Plus, consider the fact that the industry average for email address churn is 20-30 percent per year, which means just one year after acquiring an email address, there is a significant chance that address is no longer valid.

> "Email address churn is 20-30% per year"

Emailing to a lot of invalid addresses will likely result in filtering and blocking, preventing your email from reaching the inbox. So before emailing to addresses for the first time, perform a list hygiene cleanse with the help of an email address validation vendor—such as Fresh Address or Brite Verify—to identify known bad addresses.

Four Quick Tips

1. Require double email field confirmation.
2. Consider using an email validation vendor to clean out known hard bounces before you send for the first time.
3. Send a welcome message or series to communicate clearly and reinforce subscriber expectations.
4. Don't incent sales associates for email signups. This leads to very low quality entry.

Email address validation vendors have proprietary list audit technology, which helps reduce bounce rates by flagging invalid email addresses, including:

- Duplicates
- Typos
- Formatting problems
- Syntax errors
- Dead domains
- FCC-mandated wireless blocks
- And the DMA's "Do Not Email" records

Where possible, they also flag bogus and malicious email addresses—as well as some spam trap and honeypot addresses—to help minimize support issues and keep you off of blacklists.

The Wrong Way to Collect Email Addresses

As mentioned previously, it's not a good idea to incent sales associates for email signups as it leads to a very low quality of email addresses entered.

Here's why:

- Sales associate misunderstands the correct email address.
- Customer gives a fake email address to get the offer.
- Customer might not know their correct email address or provides an old address they no longer use.
- Sales associate or the customer mistypes the email address.
- Customer doesn't understand they will receive promotional email.
- Customer who receives any email beyond an eReceipt is often surprised.

Acquiring new email addresses is of course the golden goose for marketers but experts point out that there are inherent dangers: New signups risk a Spamhaus listing because emailing multiple times to a new registrant who never opens or clicks is a high risk gamble. This newly acquired email address can likely be a spam trap, and repeated emailing to it can trigger a blacklisting.

> "Acquiring new email addresses is of course the golden goose"

> **"List segmentation has been elevated to a new level with the availability of data from Marketing (Digital Body Language), Sales (opportunities and pipeline), and Finance (historic billings by product group) all in one place."**
> ***– Stone Mountain, Inc.***

ISP Changes

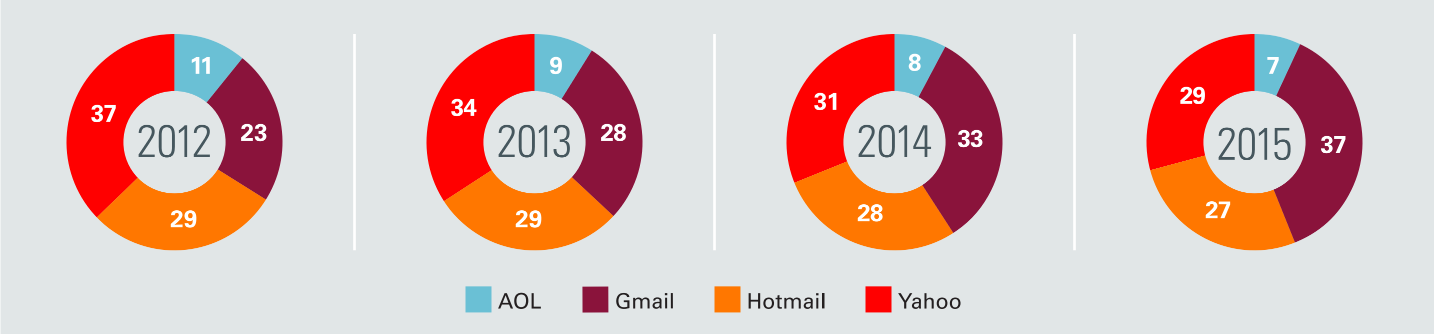
The ISP landscape is constantly changing and over the last few years there have been significant shifts in market share. ISPs are continually changing and evolving their offerings in order to provide their customers with the best services possible. Declining domains are starting to get picked up by larger ISPs and mergers/acquisitions are contributing to the shift as well.

Let's start with talking about the major ISPs. Gmail, Hotmail, AOL, and Yahoo! are still holding strong with the largest market share. However, there have been several shifts between these big four ISPs.

Based on our own internal research and data, we found that Yahoo! had the largest market share in 2012 accounting for 37 percent of volume. Jumping to 2015, Gmail now takes the lead, pushing Yahoo! to be the second largest worldwide.

AOL and Hotmail have also been on the decline. Over the years, AOL's share of overall volume has declined approximately four percent and Hotmail's has declined by approximately two percent.

Sent Volume by ISP



Gmail Changes Over the Years

Over the past few years, Gmail has made several changes to their services in order to improve their offerings and keep their customers happy. Here are a few of those changes:

- **Gmail Tabs**. In 2013, Gmail made a significant change to the user interface. The change brought in the use of tabs as a way of sorting incoming email messages. Gmail now sorts email among the primary, social, promotions, updates, and forum tabs. Personal messages arrive in the primary tab.
- **Quick Action Buttons**. Actions are buttons that are displayed in the subject line of an email. Some examples of what might appear in the buttons are: track a package, submit a review, order status and other similar things. The buttons are interesting, and can be a nice driver for your customers to get to important information quickly.
- **Easy Unsubscribe.** Gmail is now displaying an "Easy Unsubscribe" button in every email which is an expansion of the existing "List Unsubscribe" mechanism. When "List Unsubscribe" is within the header of an email, a link is embedded that sends an unsubscribe request—with the user's email address—back to the sender.

In addition to the changes subscribers witnessed for Gmail, marketers and ESPs welcomed new features that benefit them as well.

- **Postmaster Tools**. Gmail has set up a tool that gives marketers the opportunity to view specific metrics that may have led to deliverability issues. Senders get data and facts straight from the source (Gmail) and can make intelligent data-driven decisions to improve their email program.

> The ISP landscape is constantly changing

Why Are All These Changes Important?

Gmail is not the only ISP making changes. Microsoft, Yahoo!, and several others have quickly followed suit releasing several features of their own. All of these changes have been in effort to provide their customers with a satisfying email experience. They are constantly making tweaks and changes to ensure that subscribers are receiving mail they are actually interested in and sending unwanted mail to the spam or junk folder.

Staying on top of these industry trends is helpful when developing your email marketing strategy. By understanding the different features subscribers have available to them and also understanding where your audience is most, you can plan better strategies. For example, if the majority of your subscribers are at Gmail, you may want to pay close attention to how your campaigns are rendering in the Gmail web client. You will also want to understand how different features such as easy unsubscribe or quick action buttons are affecting your list retention rates.

Deliverability Strategy

Today's email marketing managers are expected to manage email deliverability. In addition to everything else that goes into good email marketing, deliverability can no longer be ignored. In fact, good email deliverability can improve email marketing performance like nothing else. Consider this: If you can deliver your email messages to the Gmail inbox, rather than the spam folder, you'll transform your email marketing program. If you can go from blocked to unblocked, you'll see huge results from your efforts.

You may think you don't have the expertise, or maybe you do and you don't have time to spend on deliverability. The good news is, many ESPs now offer Deliverability Strategy. Larger ESPs have been hiring deliverability experts and offer various levels of deliverability consulting for a price. Don't expect too much from the basic service, but support levels are included with most ESP accounts.

Deliverability Strategy engagements are typically a paid, premium service, and can be money well spent. A deliverability consultant at your ESP is already up to speed on what's happening in the ever-changing landscape such as, what spam filtering changes Gmail has made recently, for example. They will know all the tricks to pull the most effective deliverability reports out of your email sending platform. They will be able to pull data and reports much faster and more efficiently than you can, because they do this all day long. This will be a time-savings worth the expense alone, in many cases.

A deliverability consultant at your ESP will have direct access to your mail stream data, including bounces, open and click-through rates, complaint rates, unsubscribes, etc. This direct access allows your ESP consultant to provide you with real world recommendations and strategies based on your data, rather than just industry best practices.

Good deliverability strategy will help you get unblocked if necessary, but more importantly, it will help you avoid blocking and filtering in the future. Your deliverability consultant will work with you to build long term strategies to ensure your email marketing programs reach the inbox and are seen by your customers. The work of a good deliverability consultant augments the work of your email marketing team, so you can stop worrying about deliverability, and go back to being good email marketers again.

Need-to-Know-Deliverability Metrics

Most email marketers are familiar with engagement metrics such as click through rate, open rate, and so on. But, when it comes to deliverability success, monitoring engagement metrics goes hand in hand with monitoring the more traditional deliverability metrics, such as bounce rates, spam complaints, and more.

For example, there are generally two kinds of bounces—soft and hard. Identifying one from the other can provide insights into problem areas and potential root causes of deliverability issues.

Another example of a specific metric that can provide email marketers with invaluable insight is open-to-click ratio. This metric helps marketers measure just how effective and compelling their content was for the reader. Moreover, in the eyes of major ISPs, consistent engagement metrics can establish a positive sender reputation and strengthen overall deliverability.

Once an email has been delivered successfully without bouncing, there are additional measures such as delivery of emails to a recipient's inbox versus delivery to their junk/spam folder.

The bottom line is to continually monitor, react, and adjust to email marketing metrics so marketers can drive a strong sender reputation with ISPs. This ultimately allows marketers to consistently reach their audience and achieve their business goals.

> “Continually monitor, react, and adjust”

Breaking Down Bounce Rates

Let's take a deeper dive into a couple of the email deliverability metrics.

First, bounce rates—when an email is sent but then returned with a notice that the message was not delivered. There are two types of bounces—a hard bounce and a soft bounce. The main differentiator between the two is that hard bounces are permanent and emailing to them should not be attempted again, whereas soft bounces are temporary and can be retried. The world would be a much simpler place if all soft bounces were temporary and all hard bounces were permanent. But such is not the case as different ISPs handle bounces in different ways. There are two standard bounce classifications that differentiate between hard and soft:

Generally speaking, bounces that begin with a 4xx explanation are considered soft or transient delivery failures. This means they can be reattempted for delivery and may still have a chance of being accepted by the receiving domain at a later time.

If a bounce begins with a 5xx code and message pertaining to a permanent failure, then it is considered a hard bounce. Reattempting delivery of these bounces is not likely to succeed and may in fact do further damage to a sender's reputation.

Experts say that it is very important to note that should you retry sending emails to hard bounces, you not only run the risk of affecting your reputation as a sender, but also impacting overall deliverability. It is also worth noting that bounced emails for campaigns are captured in bounce tables and should be analyzed regularly to look for unusual issues, trends, and to periodically purge your lists.

Explaining Spam Complaints and Traps

Next, the omnipresent spam complaints, which are based on abuse reports received from the ISPs currently offering feedback loops. Spam is figuratively and literally a four-letter word for email marketers, and spam complaints are indeed a major factor in determining inbox placement.

The reasons why someone clicks the spam button are numerous, including they simply don't want to receive your message anymore and for whatever reason don't click unsubscribe or they received an email that was not expected or came from a brand they did not recognize or authorize.

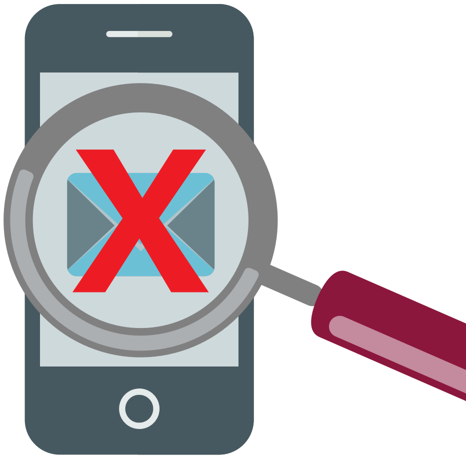
Regardless of why and when recipients hit the spam button, even in small numbers, the sender reputation dips, resulting in messages being filtered to the bulk folder and sometimes resulting in delayed or blocked delivery.

Experts recommend measuring your spam complaint rates on a daily basis and also looking at seven day and 30 day rolling windows. Keep in mind that not all ISPs report back user spam complaints. Gmail, for instance, does not provide spam complaint data. Windows Live Hotmail/Outlook.com, Yahoo!, AOL and others do provide this via feedback loops.

Under the guise of one size does not fit all, it is important to review spam complaint rates at each individual ISP in order to gain an understanding of how user behavior and deliverability varies across email providers. One of the most damaging issues for email deliverability and maintaining proper list hygiene are spam traps, and avoiding them. There are two types of spam traps:

1. **Recycled Spam Trap**. An old or inactive email address that has been kept alive for the sake of catching senders who continue to email non-existent or unengaged subscribers.
2. **Pristine Spam Trap.** This exists for the sole purpose of catching spammers who should never have acquired this email address in the first place. The pristine spam trap never subscribes or opts-in to any kind of marketing communications. Avoiding these spam traps requires diligent monitoring of engagement levels and removing inactive subscribers. Experts say that while any type of spam trap hits are damaging to a sender's reputation, pristine trap hits are exponentially worse.

Bulking, Blocking, and Blacklisting



When a sender starts to notice poor performance with their email program due to a deliverability related issue, it is likely that the sender is being be bulked, blocked, or blacklisted. Although all three terms stem from similar reputation related issues, it is important to note that there is a distinguishable difference between how each affects your program.

Bulking

Occurs when an ISP accepts your mail but routes the message to the BULK or SPAM folders vs. routing it to the INBOX.

Senders will often utilize a third party service that gives insight into inbox placement rates based on seed addresses and panel data.

You should also analyze your open rate trends over time. Significant decreases could indicate bulking.

To improve bulking issues, leverage available data to create highly targeted content. Send to an engaged audience and focus on subscribers that have opened/clicked within the last 12 months. Finally, be conscious of your frequency. Mailing too frequently will cause the majority of your mail to go unopened and will decrease your engagement rates.

Blocking
Occurs when an ISP takes action and refuses to accept your emails by bouncing them back.

Stems from poor IP reputation.

Analyze your bounce rates for each ISP. High hard bounce rates can hurt reputation and contribute to a block. However, the actual indicator for blocking would be a high soft bounce rate.

To improve blocking issues, utilize engagement based filtering to focus on your engaged segments. Send email on a consistent basis and at the right frequency and introduce new subscribers through a welcome program so that you can set expectations up front.

Blacklisting
Occurs when your IP has been flagged for sending unwanted traffic and followers of that blacklist decide to block your emails.

Being listed on a significant blacklist such as Spamhaus will cause your delivered rates to drop dramatically at the major ISPs.

High bounce rates could indicate you may be on a blacklist.

To improve blacklisting issues, implement a double opt-in component for risky acquisition channels. Utilize engagement based filtering and regularly keep up with list hygiene through the use of re-engagement and re-permission programs.

Whether you are being bulked, blocked, or blacklisted the key takeaway is to ensure you are following best practices by targeting your sends and sticking to your engaged audience. Don’t wait for an issue to surface. It is important to proactively keep up with proper list hygiene and regularly remove inactive subscribers from your list.

Onboarding for Success With a New ESP

Changing ESPs can be a stressful experience for any email marketing professional. Regardless to which ESP you’re migrating your email programs, you need careful planning and execution. From a deliverability perspective, you’ll be getting a new IP address and sending your email campaigns from a new infrastructure. Receiving ISPs track sender reputation predominantly by IP address. So switching to a new ESP means starting over with building your sender reputation.

Here are some key deliverability considerations when migrating to a new ESP.

Warming Up Your IP Address

Like going on a first date, you only have one chance to make a good first impression with ISPs. Successful warm up starts with establishing a good sender reputation over the first several days of emailing. Let's use the analogy of someone who has no credit history going to a bank for loan. Since you have no standing, the bank will naturally be suspicious of your ability to repay the loan. The same basic logic applies to how your new IP is treated by the respective ISP filters. You have to establish your reputation as a good email sender before the ISP filters will allow you to send your email campaigns without interruption. Warming up your IP address improves delivery performance, establishes credibility with ISPs, and builds your reputation as a legitimate email sender.

So what can you do?

You can start with selecting a few email campaigns that typically perform well—campaigns that usually have high open and click through rates. Starting with your best performing campaigns will begin to train ISP filters to see that the email you send is well received by your subscribers. In addition to selecting your best campaigns, segment your audience to include only your most engaged subscribers. ISPs tell us they want to see emails sent to a small, highly engaged audience—at volume levels they have prescribed—during the first days of IP warm up.

> “Ramp up volume gradually”

The best way to do this is to segment your audience by how long it's been since a subscriber has opened or clicked on an email message from you. During the first week of sending from your new IP, only send to addresses that have opened or clicked on a message from you recently—in the past three months for example. The specific criteria will vary for each sender—based on size of your email list, etc.—but sending only to recently engaged subscribers is critical during the warm up period.

After the initial warm up, you need to ramp up volume gradually over the course of four to six weeks for high volume senders. If you increase sending volumes too quickly from day to day, you may run into ISP volume triggers. Ramping up your sending volume over time will establish a volume profile, and allow you to reach your regular sending volumes.

Common Pitfalls to Avoid During IP Warm Up

The road to IP warm up wonderland, as it were, is filled with potential hazards and email marketers need to be aware of these at all times. From our experience, the most common pitfalls to avoid during IP warm up include: low subscriber engagement and high spam complaints, too many hard bounces, and increasing sending volume too quickly.

Here's how to avoid these common pitfalls:

While building sender reputation on your new IP address, send to a small, highly engaged audience. Send your most relevant email campaigns, and send only to people who have opened or clicked on an email message recently. This is critical. By sending to a highly engaged audience, you'll also be keeping spam complaints and spam trap hits to a minimum.

Exclude new signups from any campaigns you send during the first week of the warm up process. While new signups usually have high open rates, they also have high hard bounce rates and may include spam traps that will hurt your fledgling sender reputation.

Insist on porting over all suppression files from your previous provider. Any address that hard bounced, unsubscribed, or complained on your previous platform must remain suppressed. High hard bounce (invalid) rates are the fastest way to trigger filtering and blocking on your new IP.

Ramp up sending volume slowly and in gradual increments. At the end of an official IP warm up period, your sender reputation is nascent. Think of your new IP like a newborn that needs your protection. Jumping to full volume too quickly will trigger blocking and filtering, destroying the reputation you've worked hard to build.

Do Transactional-Only Email Streams Require a Traditional IP Warm Up?

Transactional-only email streams do not require a traditional IP warm up, and there are a couple of reasons:

Transactional email usually performs well with regard to sender reputation, so we don't see the typical deliverability problems associated with warming up a new promotional IP.

You cannot plan and control transactional email streams the way you can with promotional, where you select specific campaigns to use for warm up, specify segmentation criteria, etc.

Email senders typically see good delivery rates on new transactional IPs through what we call an organic warm up. Transactional email streams that are truly transactional—like order confirmations, shipping notices, etc.—should have high engagement and build a good sender reputation from the first day of sending from the new ESP.

The one caveat to consider for warming up a transactional-only IP address is to consider how quickly sending volume will build on the new IP. Rather than switching everything over to the new platform on day one, it is better to migrate a few transactional programs over to your new ESP during the first week of sending. This way, the volume builds over the first week and doesn't spike too quickly on the new IP.

Email Authentication 101

One definition of the word authenticate is "to conclusively establish the authorship or origin of." That's precisely what email authentication is all about as it validates and establishes the authorship, or identity of the email sender as a means to combat forgery and fraud. Vital to the security of your brand, email authentication helps to significantly reduce the effectiveness of two differing kinds of attacks: spoofing and phishing. Based on their individual policies, ISPs may require some or all of the authentication measures that are available.

All ESPs will ensure their systems are configured correctly, and all authentication protocols are in place on their end. However, when setting up a new account, new senders need to be aware of the requirements on their end to make sure authentication is correctly configured everywhere it needs to be. Your ESP set up documentation should explain your obligations in detail.

These are the key measures of email authentication used today:

- SPF. The Sender Policy Framework (SPF) is an open standard method to prevent sender address forgery. It enables the verification of a sender's IP address by crosschecking the domain in the "Mail From" line of an email against the published record a sender has registered in the Domain Name System (DNS).
- DKIM. Domain Keys Identified Mail (DKIM) provides a method for validating whether an email message was sent by an authorized source. DKIM utilizes cryptographic authentication. It requires a sender's computer to generate public/private key pairs and then publish the public keys into their Domain Name System (DNS) records.
- DMARC. Domain-based Message Authentication, Reporting, and Conformance (DMARC) standardizes how email receivers perform email authentication using both of the well-known SPF and DKIM mechanisms. This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo!, and any other email receiver implementing DMARC.
- TLS. Transport Layer Security (TLS), is a protocol that encrypts and delivers mail securely. It helps to ensure no third party can intercept and tamper with an email message. TLS is designed to prevent eavesdropping and spoofing (message forgery) between mail servers. TLS is a standards-based protocol based on Secure Sockets Layer (SSL), and is rapidly being adopted as the standard for secure email. The protocol uses cryptography to provide endpoint authentication and communications privacy over the Internet. TLS is the email equivalent of HTTPS for web communications and has similar strengths and weaknesses.

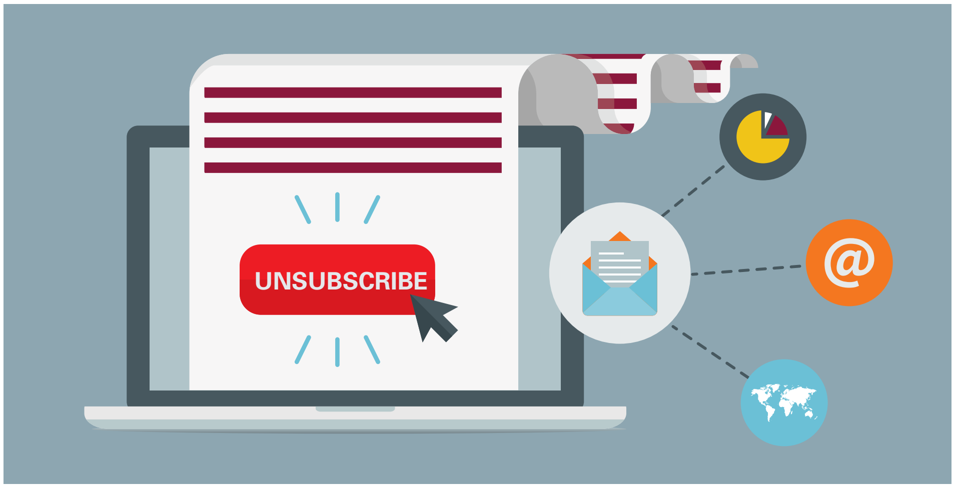
Feedback Loops

When setting up accounts, you also need to be aware of feedback loops (FBLs). FBLs play a major role in overall email deliverability. One of the greatest tools we have in managing reputation and email deliverability is feedback from our recipients. Many ISPs provide us with just that via FBLs, which provide a path used by the ISPs to relay information (feedback) they receive from your recipients back to us. When a subscriber clicks on a spam or junk button, reporting an email as spam, this information is then recorded by the ISP and provided to us through the current feedback loop set up. Feedback loops are offered by many of the well-known ISPs:

- AOL
- Bluetie
- Comcast
- Cox
- Earthlink
- Fastmail
- Terra
- Rackspace
- Synacor
- USAnet
- Hotmail
- Roadrunner
- Yahoo!
- Zoho

> "Be aware of feedback loops"

You will notice one glaring omission from this list: Gmail. Unlike most major ISPs, Gmail does not offer a feedback loop for processing spam complaints. However, they do make another feature available for senders to be able to collect and unsubscribe recipients who have marked their messages as spam called List-Unsubscribe or a more endearing name might be The Poor Man's Feedback Loop.



Gmail's List Unsubscribe

To implement List-Unsubscribe at Gmail, you must:

- Authenticate email using SPF or DKIM.
- Have good sender reputation at Gmail.
- Use the mailto: option with the List Unsubscribe header. The email notifications from Gmail would then be sent to the mailto: address.

The Truth About Whitelisting

Currently, only AOL and Yahoo! manage an actual whitelist. Whitelisting is a way for senders to assert they are following best practices, and should be trusted by the ISP. There is no guarantee of inbox delivery, or even a way to know if you remain on the whitelist. There is minimal to no benefit to legitimate email marketers for being on either of these two whitelists, since filtering rules will be imposed on each email campaign you send out. Whitelisting is not a free pass to someone's inbox.

It is, rather, a declaration to an ISP that you will be sending high volumes of email from a particular IP address. Most ESPs will sign you up for both the AOL and Yahoo! whitelists as standard procedure, but there are mailing history requirements, so expect a delay when signing up too early.

Secrets to New Subscriber Engagement

Personalizing your marketing based on customer data such as channel preference and purchase history is what fundamentally drives high engagement with emails. And, the need to keep your subscribers engaged takes on a whole new meaning and level of importance when it comes to the topic of deliverability since a lot of the major ISPs are looking at and monitoring user-level engagement to determine inbox delivery.

The more sophisticated marketers become in personalizing individual customer experiences, the more relevant email messages become, which drives more engagement and more inbox placement versus junk folder placement.

Opens and clicks—and the recency of those activities—is often the metric used to determine email engagement level. When those in your database become uninterested and stop clicking on your emails, there can be adverse effects on email deliverability.

The bottom line is that by continuing to send email to unengaged subscribers, you're putting your reputation as a sender at risk, as well as increasing the chances of an inactive address being converted into a spam trap.

Defining Engagement

So how do you define engagement? Experts say that often clients have an internal definition of an active customer and inactive customer that have to do with website visits, purchase history, customer or account status. While these definitions make perfect sense from a business standpoint, from a deliverability standpoint they have little bearing.

ISPs need to see engagement with email specifically.

ISPs have gone on the record saying that they track user activity in two categories: positive engagement and negative engagement.

From a deliverability perspective, clicks are the only fully accurate measure of activity for an email recipient because a click is a definitive action taken by the recipient. Opens are secondarily helpful as an engagement metric, although there are potential inaccuracies with opens because of preview pane usage and image suppression.

“Clicks are the only fully accurate measure”

Recipient actions that contribute to a positive engagement quotient are:

- Clicking through links
- Adding an address to their contacts or address book
- Enabling images
- Opening the message
- Scrolling through the message

Recipient actions that contribute to a negative engagement quotient are:

- Reporting as spam
- Deleting the message
- Moving the message to trash
- Marking messages as read
- Ignoring messages

Extended Buying Cycle Consumers

There are various types of businesses that fall within the extended buying cycle (EBC) category. Examples of purchases would be business technology, luxury items, or large household appliances.

Since the period in between purchases can be quite long, it’s important to monitor your subscribers to ensure the email addresses are still active. Without regularly communicating and monitoring engagement, your list may start to fill up with bad addresses and uninterested subscribers that are likely to complain. A build up of old/inactive addresses could also lead to spam trap issues.

The goal is to find an effective communication strategy to keep subscribers interested without overwhelming them. It’s also important to recognize the right time to remove certain subscribers from your list.

Messaging Types

Make sure your messaging is targeted and personalized when possible. Examples of the types of messages you could send include:

- **Promotional** – Offer driven with sense of urgency
- **Service** – Customer service/satisfaction
- **Educational** – Information for the customer regarding their purchase
- **Brand Value** – Reinforces brand benefits and value
- **Transactional** – Provides information related to a specific purchase

Timing is critical for deciding the type of message to send. For example, if a consumer just made a large purchase and is not likely to purchase again for several months, then sending a promotional message may be irrelevant. Instead, you could send an educational email reminding the customer of the product benefits.

How to Approach Inactivity

The potential downside to these metrics comes in the form of inactivity. Yes you want to put your customer front and center but what if, for example, over half of your distribution list has neither clicked nor opened a single email in one year? That could have major ramifications according to experts who say they've seen major ISPs filter all the incoming email, even email going to engaged subscribers.

And size does matter. ISPs tolerate even less inactivity from high-volume senders. They will begin to send unengaged email recipients to the junk folders from senders with list sizes in excess of one million.

When it comes to the duration of inactivity, ISPs each have their own tolerances for how long an address can go inactive, but in general any activity inside of 12 months is acceptable. You'll want to develop segments specific to your own program. As a high level recommendation, you could group your subscribers into four engagement based segments:

- **Most Active** – Opened or clicked in the last 3 months
- **Lapsing** – Opened or clicked in the last 3-6 months
- **Lapsed** – Have not opened or clicked in the past 6 months
- **Inactive** – Have not opened or clicked in the last 12 months

Of course, this recommendation should be tempered by the percentage of the marketer's list that's inactive, in addition to their sender reputation. If a large percentage of a list is inactive, the acceptable duration of inactivity decreases.

Decreasing the frequency at which inactive subscribers are emailed is a defensive tactic used to boost the level of engagement seen by ISPs, while continuing to give these subscribers opportunities to engage. Once a definition of inactivity is in place, the next step is to make changes in the messaging or frequency as part of a reengagement strategy.

Create a Plan for Reengagement

The success of a reengagement program is characterized by opens and clicks. If inactive subscribers don't respond to reengagement efforts, eventually they should be removed from mailing lists because of the deliverability dangers.

As a last-ditch attempt to save inactives from being removed, some marketers may find nominal success by taking the intermediate step of sending a re-permission campaign. These emails ask a subscriber to confirm their continued interest in receiving emails by a certain date or be removed from future mailings.

From a deliverability perspective, re-permission campaigns are needed when a sender is being heavily junk foldered (80 to 90 percent or more) at any given ISP for an extended period of time (more than one to two weeks) and inactivity or spam traps are the root cause of the junk foldering. In order to identify the audience that should be sent a re-permission email, a full inventory of actives versus inactives, and business terms and time tables for each must be established.

Then, it's important to create a reengagement strategy that uses changes in email frequency and content to keep subscribers from becoming inactive. And finally, establish rules for removing inactives from mailing lists and consider creating a triggered re-permission campaign to give wayward subscribers one last chance to stay opted-in.

Understanding International Deliverability

If you are sending email marketing messages today, chances are very high that you are sending to at least more than one country. Just because you think that you know the laws, regulations, and best practices in one country, does not mean that they will be the same in others. The email marketing landscape today is a mish-mash of different rules and regulations in each country in which you have customers. Understanding those differences is critical to success—and sometimes operational survival.

Let's say for example you have the ability to create email marketing campaigns in Chinese. How do you know if the Chinese email servers will even allow for your email to be delivered? Or what happens if your email in French does get delivered, how do you know if the PC or mobile phone in France correctly displays your message?

Experts say that to operate in today's global environment, marketers need to understand more than just email deliverability in the US. Modern Marketers should at least be aware of the privacy laws and regulations in the countries where they want to deliver email. Knowing how to operate on an international scale is vital, especially when you consider the fact that total worldwide revenues from email will grow to over $12 billion by 2016 and email traffic is estimated to grow to over 192 billion emails sent per day in the next year.

> “Knowing how to operate on an international scale is vital”

Take a Wider View of the World

US-based mailers mistakenly believe that CAN-SPAM is a good base for understanding international email regulations. In reality, CAN-SPAM is one of the least restrictive set of regulations. CAN-SPAM doesn't have many address collection rules. The stipulations and penalties mostly deal with allowing recipients to opt out. However, many other countries have much stricter laws governing permission and what is necessary for lawful contact. Australia is a great example of a place with dramatically different feelings about permission. The Australia Communications and Media Authority (ACMA) take dramatic steps to prohibit unsolicited emailing. ACMA will take out front page ads in major Australian newspapers to shame violators.

Heavy fines are common for practices that are acceptable under the US version of CAN-SPAM. A good rule of thumb when emailing to domains outside the US is that explicit permission will be required, even with transactional email. Many senders incorrectly believe that transactional email is exempt from any repercussions. While transactional email does often fit into different legal categories, as far as receivers are concerned, all email is the same.

Experts say there is no special pipe or identification for this type of transactional message. Yahoo! or Hotmail for example see a transactional message the same way they see a newsletter.

This means that you must still build and maintain a strong sending reputation to actually deliver these messages. This is especially true for international domains because the volume is generally smaller.

The Canadian Anti-Spam Legislation (CASL)

CASL (Canadian Anti-Spam Legislation) went into effect on July 1, 2014. This law isn't just for Canadian based senders. CASL has an impact for anyone who communicates with any Canadian residents. The law is certainly a step beyond the US CAN-SPAM law in many respects. The main differences are around the gathering of specific types of permission.

CASL contains potentially stiff penalties, including administrative penalties of up to $1 million per violation for individuals and $10 million for corporations (subject to a due diligence defense). Several fines have already been levied in the first year. CASL will eventually set forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL ($200 for each contravention up to a maximum of $1 million each day for a violation of the provisions addressing unsolicited electronic messages).

There are three main requirements with CASL:

1. Get consent (express, implied, prescribed information).
2. Identify all senders.
3. Provide an unsubscribe mechanism.

The European Union

There are two levels of legislation to consider:

1. The Umbrella EU legislation that applies to all member states.
2. The individual country level requirements that vary from member state to member state.

Consent requirements do vary from region to region. However, many do require not only that consent is explicit but also require proof of consent to be stored. When you have areas such as the EU where there are several layers of regulation and local requirements that may not apply to all, it makes sense to implement strategies that ensure you are compliant across the board instead of attempting to meet each individual area's requirements. You can do this by identifying the individual region with the strictest requirements and ensure you comply with these.

> "Consent requirements do vary from region"

The Importance of China

Understandably, emailing to consumers in China is becoming increasingly important for many marketers. However, marketers must take time to understand the country's deliverability landscape in order to be successful.

Experts say it's very important to understand that deliverability success in China is measured in different ways than most senders are familiar with. Open rates are one area that should be measured differently. The global open rates of major ISPs are around 25 percent. However open rates are substantially lower in China. So if you have an open rate of say 12 to 15 percent in China that does not necessarily mean your campaign did not fare well. The regulations and real-world requirements for mailing to Chinese domains are also very different from other regions. The technical requirements and permission standards are much more difficult than global domains such as Yahoo!, Hotmail, and AOL.

Filtering tends to be set up as you might have expected to see in the US three to five years ago. Generic messages do not tend to perform very well. Be sure to send individually relevant information whenever possible.

One massive difference from big global ISPs is the warm up period. This warm up process typically takes 30-45 days with most ISPs. The ramp up with Chinese ISPs like Netease and Tencent/QQ can take several months to get to full volume.

Global Deliverability Tips

Argentina — Explicit consent is required. Argentina has a public do not contact list—the DNPDP—that must be honored.

Australia — Explicit consent is a must. Very strong laws regarding permission and data privacy. Australian ISPs are very responsive to consumer issues.

Belgium — Opt-in is required and the sender is responsible for refer-a-friend consent and managing those opt-outs, making this practice dangerous.

Finland — All marketing messages must be clearly marked as advertisements

France — Consent is required for emailing. French ISPs historically accept fewer connections making email delivery times slower.

Germany — Strong laws requiring opt-in. If a recipient opts-out of a mailing, all data must be erased from the sender's database.

Hong Kong — Expressed consent is required and it must be different from T&C acceptance. Consent must be clearly differentiated and easy to understand.

Italy — Prior consent required for marketing messages. End-user consent is required for cookie use and senders must disclose if any data will be shared with a third party.

Netherlands — Pre-checked boxes are not allowed as a mode of consent.

Russia — There are no current electronic privacy laws. Russian ISPs such as mail.ru can be challenging. Having a local business presence is very helpful. ISPs like Yandex have begun offering senders new insight into campaigns.

Spain — Maintains a government do not mail list.

Japan — All email must contain clear and visible information for sender name and title, correct address for an opt-out (must be at the top of the email) and the sender's address and phone number must also be displayed.

Canada — The Canadian Anti-Spam Legislation (CASL) took effect July 1, 2014. The full provisions roll out over three years. Explicit permission and private right of action are the most important measures.

Singapore — All messages must contain an unsubscribe link, phone number, and a postal address. This information must be in English. Unsubscribes must be handled within 10 days.

About Oracle Marketing Cloud

Modern Marketers choose Oracle Marketing Cloud solutions to create ideal customers and increase revenue. Integrated information from cross-channel, content, and social marketing with data management and activation along with hundreds of app and data partners enables them to target, engage, convert, analyze, and use award-winning marketing technology and expertise to deliver personalized customer experiences at every interaction.

Visit oracle.com/marketingcloud