

PATRICK M. CLAWSON  
PO BOX 470  
FLINT, MI 48501-0470  
Phone: (810) 730-5110  
Fax: (810) 963-0160  
E-mail: patrickclawson@comcast.net

August 3, 2015

Larry Royster  
Clerk of the Court  
Michigan Supreme Court  
PO Box 30052  
Lansing, MI 48909

**Re: ADM File No. 2014-40      Proposed Amendment of Rule 2.506 of the  
Michigan Court Rules**

Dear Mr. Royster:

I comment concerning the Court's Proposed Amendment of MCR 2.506 in my capacity as the President of the **Michigan Process Servers' Alliance (MPSA)**.

I submit these comments in compliance with the Court's time standards as per MCR 1.108(1), since the Court was closed for business on August 1, 2015.

The Michigan Process Servers' Alliance represents process servers and court officers across Michigan. MPSA members serve civil process on a daily basis and have long professional experience in doing so

***MPSA opposes the Proposed Amendment on the following grounds:***

- 1. Current e-mail technology is not reliable for service of process;***
- 2. The Proposed Amendment will create an unnecessary and costly compliance nightmare for law enforcement agencies and litigants; and***
- 3. The Proposed Amendment does not adequately protect the constitutional due process rights of citizens.***

**E-MAIL TRANSMISSION IS NOT A RELIABLE  
METHOD FOR SERVICE OF PROCESS**

The Proposed Amendment would allow service of subpoenas on various government agencies, law enforcement agencies and "accredited forensic

laboratories" (apparently including private non-governmental laboratories) via electronic means, including e-mail. If a confirmation message is not received from the served party within 48 hours, conventional means of service would be required.

While MPSA supports the use of modern technology to improve the administration of justice, the fact is that electronic mail technology is not yet reliable enough to ensure that service of critical legal process such as summonses and subpoenas has been completed successfully and that due process notice requirements have been met. While laymen perceive email to be fairly reliable, the reality is that e-mail messages frequently get lost in cyberspace and are undelivered.

Return Path, the leading e-mail marketing consulting firm, has for several years published annual studies on the reliability of e-mail inbox delivery for commercial marketers. Its 2014 report, the latest available, states:

***"For every six commercial messages sent worldwide, one never reaches the subscriber's inbox. It's diverted to a spam folder or missing altogether, probably blocked by the mailbox provider."***  
(Source: *Inbox Placement Report, Return Path Benchmark Report 2014*)

Return Path has made similar findings in its annual reports for **each of the past five years**. A copy of the 2014 Return Path report is attached to this letter.

There are four key points to be considered about e-mail technology:

- ✓ Email can be lost without any bounce-back message to the sender.
- ✓ The timeliness of an email traveling from sender to receiver is unpredictable at best.
- ✓ The reliability and timeliness of an email is directly related to the sending and receiving email providers, and the time of day.
- ✓ Email reliability and delay problems are not limited to Internet Service Providers but also exist in government and private business IT-managed email systems.

Even when e-mail is transmitted, it can often take hours or days to reach the recipient. This is due to the store-and-forward nature of e-mail and the use of e-mail spam filters by Internet Service Providers. Under current technology, the responsibility for delivering email passes from one mail server to another. This exposes messages to loss if a server fails, malfunctions or unduly restricts its delivery. As one technical source puts it:

***"Internet email system is a non-confirming delivery protocol, which means that there is a no guarantee that an email sent from you will be delivered to the intended recipient(s). We assume that an email will be delivered to a recipient if no "undeliverable" message is returned to you. However, this is not a safe assumption as large ISPs do filter email messages without returning "undeliverable" message (email blackhole)."***

(Source: <https://www.iplocation.net/email-delivery-problems>)

## **ANTI-SPAM FILTERING IS AN INCREASING PROBLEM FOR E-MAIL DELIVERY**

A primary reason for e-mail unreliability is that Internet Service Providers are constantly adjusting their e-mail technical delivery parameters to both block spam and to update for new technologies. Further, there is no universal or common standard for the use of these blocking technologies. Each ISP uses its own methods, including proprietary software and technology that is not compatible with that used by other vendors.

The increasing use of spam filters by major Internet Service Providers such as AT&T, Comcast, Charter, Frontier and Verizon is having a demonstrable effect on the ability to successfully deliver e-mail. A research paper by Microsoft engineers states:

***"The Internet SMTP-based email system does not guarantee the timely or even eventual delivery of messages. Email can sometimes be delayed by hours or days, or even fail to be delivered at all to the recipient(s). The email sender isn't always notified when such failures occur. Such silent failures, even if rare, impose a high cost on users in terms of missed opportunities, lost productivity, or needless misunderstanding (notwithstanding the purported social "benefits of plausible deniability offered by email loss)....."***

***Email could be delayed or lost because of overload, failure (e.g., disk crash), or upgrade of a server along the end-to-end, store-and-forward path from the sender to the recipient. Overload or failure is sometimes triggered by a spurt in the volume of email because of spam or the spread of a virus. Furthermore, the widespread use of spam filters also contributes to email loss by sometimes causing legitimate emails to be discarded as spam. For example, from conversations with the IT staff at a major corporation, we have learned that an estimated 90% of incoming email is dropped even before these hit the user mailboxes or junk mail folders, typically to reduce storage and processing costs for the mail server. Given such***

***an extensive discarding of email, it is hardly surprising that some legitimate email might be caught up in it."***

(Source:<http://research.microsoft.com/enus/people/sagarwal/hotnets05.pdf>)

Other technical problems may arise in the form of "false positives" or erroneous indications that an e-mail has been successfully transmitted. False positives add unintended risk to those business processes which rely on email messaging. They impact the integrity of such processes. Many organizations are unaware of the actual level of risk that their spam filters are causing right across their agencies or businesses every day. As one source has noted, e-mail delivery false positives are often a two-step process:

***1. 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.***

***2. 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.***

(Source: [https://www.trustsphere.com/wp-content/uploads/2014/08/Restoring-reliability-deliverability-and-integrity-of-email-communications\\_20120802.pdf](https://www.trustsphere.com/wp-content/uploads/2014/08/Restoring-reliability-deliverability-and-integrity-of-email-communications_20120802.pdf))

## **USE OF E-MAIL ATTACHMENTS INCREASES RISK OF NON-DELIVERY**

Based on the current daily professional experience of Michigan process servers, the most likely way an attorney would electronically submit a subpoena to an agency would be in the form of an e-mail with an attached file (such as a PDF file) containing the actual subpoena. This is the same form as many commercial e-mail messages.

Anyone transmitting an e-mail attachment faces an increased risk that their e-mail will be rejected by either ISP or recipient spam filters and will never be delivered.

A major reason why some Internet Service Providers fail to deliver or automatically divert e-mail to spam folders is because the e-mail message contains an attachment. In recent years, ISPs have been stepping up their policing of e-mail traffic containing attachments because of the escalating amounts of e-mail spam and viruses/malware being sent as attachments.

Several professional e-mail marketing firms now advise their clients to **never** send an attachment with an e-mail message, but rather to include a hyperlink in the body of the e-mail where a user can go to download a document. I submit

that it is unreasonable to expect over-worked law enforcement personnel to take extra steps to find and then do a secondary download of subpoenas that may be referenced in the body of an e-mail.

I note that from my own personal experience as a professional process server who uses e-mail in the course of my business that is not uncommon to fail to receive e-mailed messages and documents from attorneys. Delivery failure also occurs periodically when I send e-mails with attached documents to attorneys. In one recent case, I had to transmit an e-mail message with an attached Proof of Service six times before the attorney received it, and I finally had to transmit it to an alternative e-mail address on the system of a different Internet service provider.

In my particular case, I use Comcast as my Internet Service Provider as do many Michigan law firms and government agencies. Comcast is America's largest residential and commercial Internet Service Provider. I have complained to Comcast many times over the past decade about problems with e-mail traffic. In none of those cases have I received a satisfactory response about the cause or cure of those problems. Further, Comcast has a history of interfering with e-mail and other Internet activity of parties that have been critical of its business practices.

Also, Internet e-mail delivery is often subject to interference from self-appointed vigilantes or "spam cops" who maintain IP address blacklists that are used by major Internet Service Providers to help manage their anti-spam filtering. The criteria for being placed on these lists is vague at best, and removal for an unwarranted listing is very difficult. The most notorious of these vigilante groups is SPAMHAUS, a non-profit volunteer group that once blacklisted Amazon Web Services servers and interfered with the operations of literally hundreds of organizations that use those Amazon servers for their business. Comcast and most major ISPs use the Spamhaus blacklists to filter and block e-mail transmission through their networks. It appears to be very easy for an e-mail sender to get on the SPAMHAUS blacklist and very difficult to get off.

### **THE PROPOSED AMENDMENT WILL CREATE A BUREAUCRATIC AND COMPLIANCE NIGHTMARE**

This Proposed Amendment would also create a bureaucratic nightmare because it would require a "memorandum of understanding between the parties" detailing the use of electronic transmission technologies. These agreements would have to be in place prior to any use of electronic delivery for service of process.

Further, the Proposed Amendment would apply *to "the Michigan Department of Corrections, Michigan Department of Health and Human Services,*

***Michigan State Police Forensic Laboratory, other accredited forensic laboratory, law enforcement or government agency..."***

A quick Internet search indicates that Michigan has nearly 600 law enforcement agencies. The 1963 Michigan Constitution requires that all permanent agencies or commissions, except universities, be assigned to one of a maximum of twenty principal departments. There are hundreds of government agencies, commissions and boards operating under those twenty principal departments. Then there are the hundreds, if not thousands of "government agencies" that exist at the county, township, city and village level. Then, of course, are the myriad number of U.S. Government agencies operating in Michigan that also appear to be affected by this Proposed Amendment.

Since the Michigan Supreme Court is not proposing the creation of a model Memorandum of Understanding to be used in compliance with the Proposed Amendment, one can only imagine that Michigan's 34,000+ licensed attorneys will be free to create 34,000+ variants of such a document.

Each proposed MOU agreements would most likely have to undergo legal review and some amendment by an attorney for the agency or laboratory that would receive electronically-delivered subpoenas before any e-mail service of process could take place.

Can the Michigan Supreme Court provide the public with a Financial Impact Statement detailing the monetary burden than will be placed on the taxpayers of this state for government compliance costs with this Proposed Amendment?

**All of this needless and expensive regulatory burden can be avoided by continuing to require normal service of process for subpoenas by professional process servers, a method that is time-proven and works well.**

***THE PROPOSED 48-HOUR  
RESPONSE PERIOD IS NOT REALISTIC***

The Court's Proposed Amendment calls for service of a subpoena to be made by conventional means if no response is received from an e-mail recipient within 48 hours.

MPSA submits, based on our members' lengthy professional experience, that it is wholly unrealistic to expect overworked law enforcement personnel with limited resources to respond within 48 hours to confirm receipt of a subpoena. Law enforcement agencies often take days or weeks to respond to the most basic correspondence. Also, what happens if the 48-hour deadline falls on a weekend or holiday?

Further, it is unrealistic to expect most busy attorneys and their staffs to be able to monitor e-mail delivery of subpoenas and note whether or not a 48-hour response window from a law enforcement agency has passed. In the real world, attorneys and their staffs frequently lose track of documents and deadlines under the best of circumstances due to high case loads, multiple deadlines, illness or absence of personnel and other pressures.

**Professional process servers provide a very important safeguard and check-and-balance for the administration of justice since their only job is completing the service of civil process entrusted to their care and by making certain the Proofs of Service are filed with the courts in a timely manner. This level of service cannot be duplicated through the use of email.**

**IF ANY E-MAIL SERVICE IS AUTHORIZED,  
IT SHOULD BE ONLY CERTIFIED E-MAIL USED TO  
SUPPLEMENT TRADITIONAL SERVICE METHODS**

Some companies, such as RPOST and DOCSMIT, now offer specialized new services that provide "registered" or "certified" e-mail delivery. This form of e-mail provides independent verification of both transmission and receipt of e-mail. The cost of these services is low. RPOST charges as little as \$0.39 to send a secured e-mail. If the Court deems it wise to permit certain subpoenas to be delivered via e-mail, then any new Court rule should permit only the use of registered or certified e-mail services to protect due process rights of defendants.

However, even using these specialized e-mail services does not guarantee delivery of legal notice to a party. The party may have moved, changed their e-mail address, experienced computer failure, or had their Internet service malfunction or be disconnected.

**The Michigan Process Servers Alliance believes that e-mail should never be used as the primary means to serve critical process documents such as initial summonses and subpoenas. E-mail service should be used only in the most extreme cases, such as where a defendant is evading service by hiding or crossing state lines. Even then, it should be used only to supplement - not replace - traditional means of personal service of process.**

**CONCLUSION**

Considering the current state-of-the-art of the technology, the use of e-mail alone is not an adequate or reliable method of providing service of legal process.

The personal service of subpoenas and other legal process remains vitally important to protecting individual due process rights. It is critically important that existing service of process procedures defined by statute and court rules are followed to provide proper due process to litigants so they may defend their interests in court.

While the Court and some attorneys may believe there are speed and financial cost savings benefits to be had from e-mail service of process, MPSA believes that the risk to protection of due process rights far outweighs any short-term and minor gain. Our members are not technological Luddites who are resisting change. Our members are dedicated professionals who take protecting the due process rights of citizens very seriously.

When the Proposed Amendment is coupled with the recent enactment of legislation allowing service of landlord-tenant Notices to Quit by e-mail, it seems that Michigan attorneys and government officials increasingly view service of process to be a mere formality in the judicial process that can and should be achieved electronically with a bare-bones minimum of effort and expense. MPSA believes this view will result in the erosion of constitutional rights and protections of due process for our citizens and imperil the integrity of the judicial system.

**There is simply no substitute for the use of a trained and professional process server, a neutral human third party, who completes personal service of legal documents to ensure that citizens' due process rights are protected.**

Please find attached some supplemental reference materials to further inform the Court about reliability issues involving e-mail delivery.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'P. Clawson', with a large, sweeping flourish underneath.

PATRICK M. CLAWSON  
President  
Michigan Process Servers' Alliance  
PO Box 470  
Flint, MI 48501-0470  
Phone: (810) 730-5110  
Fax: (810) 963-0160  
E-mail: patrickclawson@comcast.net

# Inbox Placement Benchmark Report 2014



You might expect that after so many years of building email expertise, reaching the inbox is getting easier for marketers. It isn't. The same challenges that kept reputable senders from consistently reaching subscribers a few years ago are still there, joined recently by new complications that make inbox placement harder for even experienced email marketers.

Of the options available to generate stronger return from email marketing programs, inbox placement may still offer the best potential. For a typical sender whose messages aren't delivered to subscribers' inboxes one-sixth of the time, solving that problem can increase effective campaign reach by more than 20%. But understanding the evolving challenge of inbox placement - to say nothing of framing it within the dynamics of other elements of email marketing performance - is more difficult than ever.

Mail volumes continue to rise and spam tactics continue to evolve, pushing mailbox providers to constantly refine their filtering. As they take increasingly divergent approaches to keeping unwanted mail out of the inbox and incorporate more granular information into their decision making, mailbox providers have forced senders to develop more sophisticated ways to monitor and improve inbox placement. Some have; most are struggling to keep up.

By charting email marketers' recent efforts to stay connected to their customers, this report also illuminates some of the root causes of inbox placement challenges: proliferation of mobile devices, rapidly diversifying email applications, increasingly individualized mailbox provider decision making, engagement-based filtering and the declining accuracy of seed-based monitoring.

A number of senders are consistently reaching the inbox, which means they have successfully navigated each of these issues. Although maintaining high inbox placement won't get any easier for them, it's only getting harder for their weaker peers to close the gap; the inbox placement challenge is already dissolving customer relationships and narrowing some brands' chances of survival.

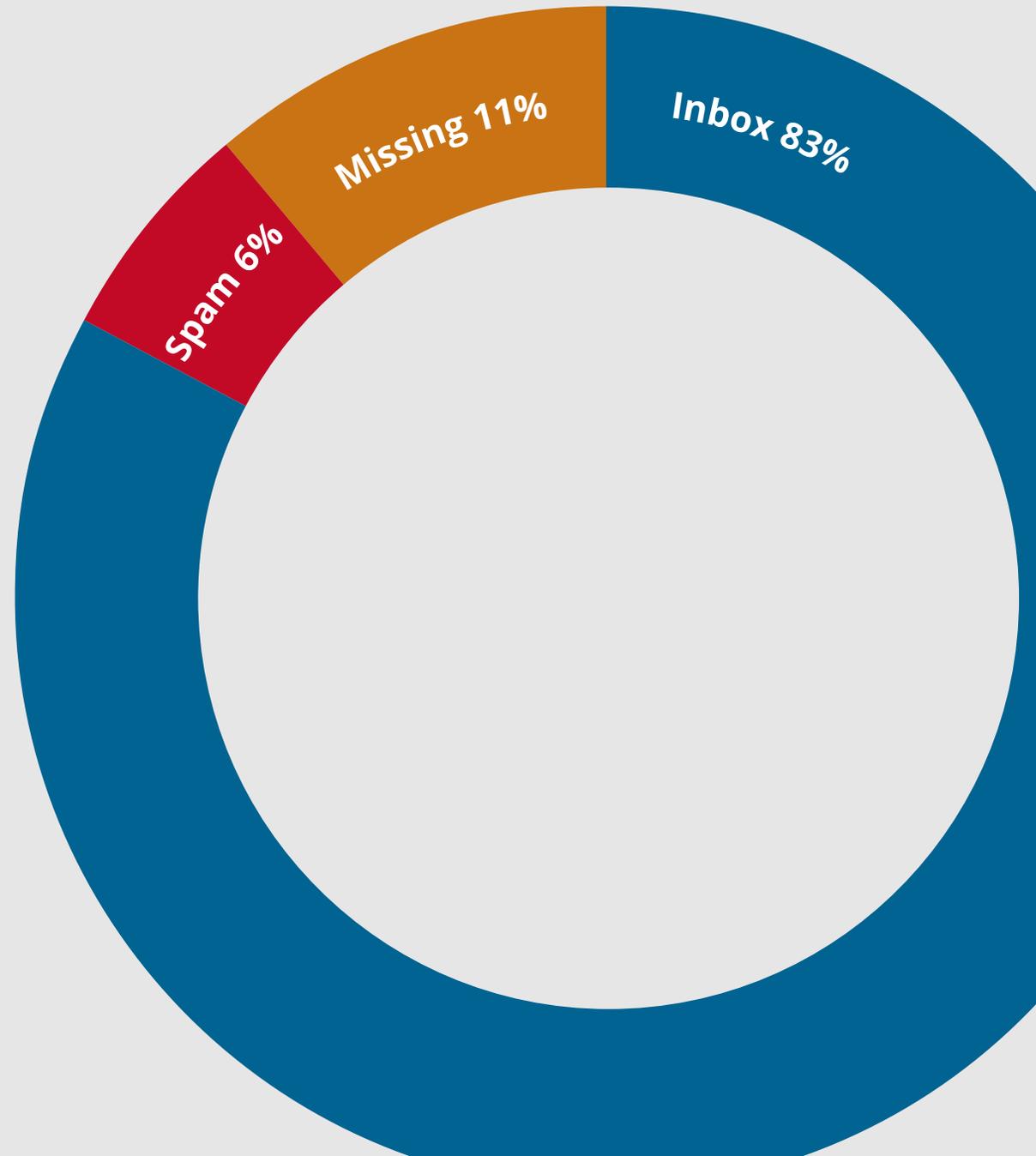
George Billbrey  
Co-founder, President  
Return Path

## One-in-Six: Inbox Placement Rates Stalled WorldWide

For every six commercial messages sent worldwide, one never reaches the subscriber's inbox. It's diverted to a spam folder or missing altogether, probably blocked by the mailbox provider.

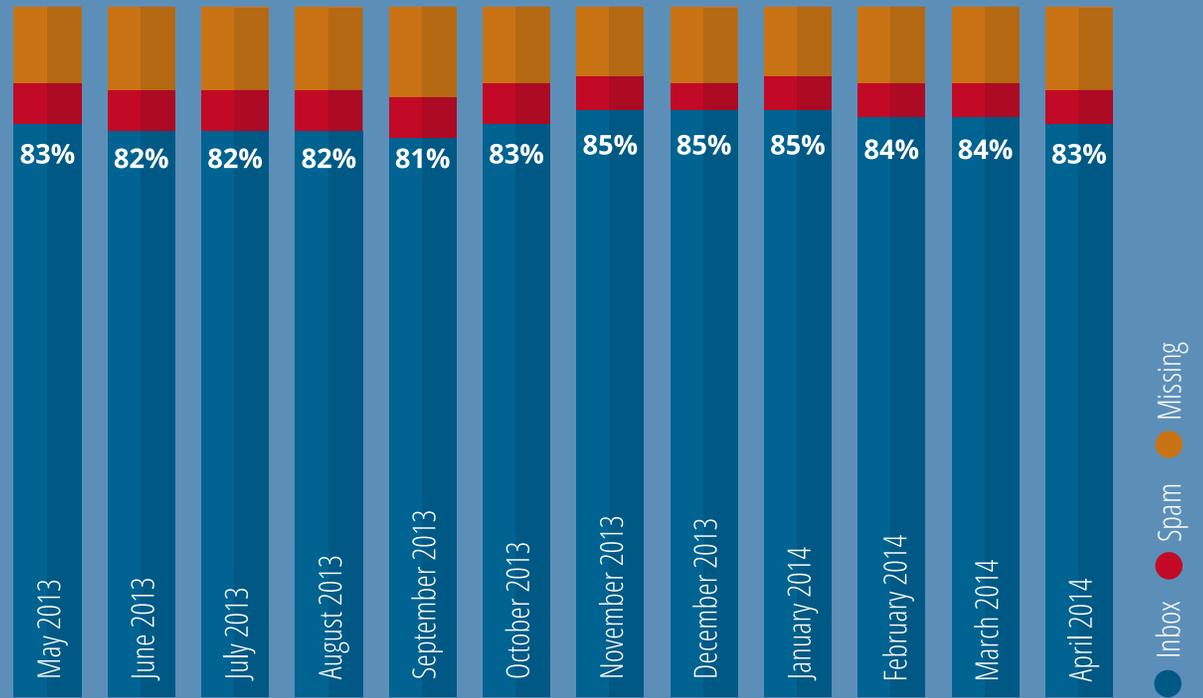
This figure includes only permissioned email from legitimate senders - email marketers that value and rely on long-term customer relationships for their survival - and it hasn't changed much over the years.

What has changed is mailbox providers' decision making, which has become increasingly complex as signals from individual subscribers play a bigger role in determining whether messages are delivered to the inbox. Best practices that once applied to broad audiences across all mailbox providers are no longer enough to ensure inbox placement, making blended averages like these less applicable to individual brands. These figures' steadiness year-over-year masks erratic performance, even within successful senders' programs.



# No Holiday Lag: Average Inbox Placement Sustained in Q4

Seasonal inbox placement trends, too, appear to be constant across the globe. In fact the one period in which inbox placement might be expected to sag - the end-of-year holiday shopping season with its huge surge in marketing email volume - generated fairly constant performance compared to the rest of the year. Three factors help explain how marketers managed to stay connected to their audiences in Q4: the amount of mail they sent, the devices they sent it to, and their subscribers' generosity.



## The Volume Effect:

Complaints as a percentage of all messages dipped as volumes climbed. As retailers in particular increased the volume and frequency of commercial email, the effect of complaints and other negative influences on reputation - and therefore on inbox placement - was diluted during the 2013 holiday season.



## The Mobile Effect:

The increase in mail read on iPhones and iPads reduced spam complaints. In November 2013, for the first time ever, more than half of all commercial email was read on mobile devices - most of which were Apple devices, whose native email client lacks a spam complaint feedback loop. Some users may have simply deleted unwanted mail because they could no longer complain easily, sparing senders any associated damage to their reputations.



## The Cheer Effect:

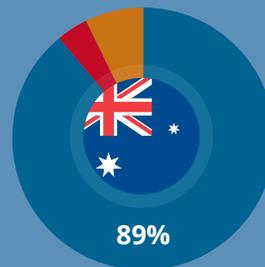
Subscriber engagement signalled to mailbox providers that consumers wanted their holiday shopping email. Subscribers may have simply been in the mood, expecting and even welcoming more promotional email. Everyone loves a good deal, especially when shopping for gifts for a multitude of people.

# Global Inequality: Inbox Placement by Country

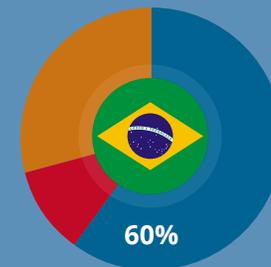
The apparent constancy of global inbox placement falls apart on a country-by-country comparison. Top-rated Australian and German senders failed to deliver one message in eight to the inbox during 2013. Meanwhile Brazilian senders struggled to stay connected to subscribers, reaching the inbox only 60% of the time, with nearly one-third of their messages disappearing altogether.

Even as bigger markets performed well, with the US and UK reaching the inbox 87% of the time, no country's marketers were able to break the 90% inbox placement threshold.

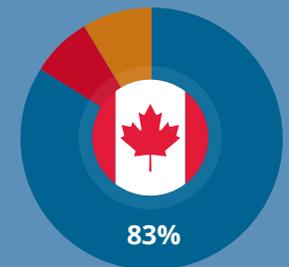
On the whole European marketers struggled more than others with missing messages, but saw less mail routed to subscribers' spam folders than North American senders did. Diagnosing and correcting problems that cause bulk delivery (to the spam folder) may be easier than tracking down reasons for missing email, but the difference isn't meaningful to a brand evaluating email marketing performance. Subscribers rarely engage with messages in their spam folders, so their contribution to marketing ROI is negligible; failing to reach the inbox, regardless of the reason, means failing to reach a customer.



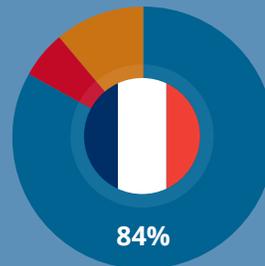
Australia



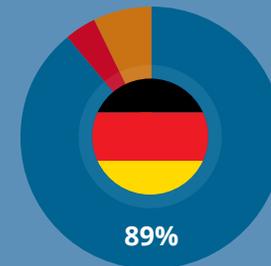
Brazil



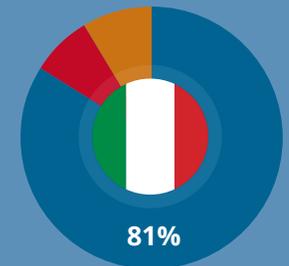
Canada



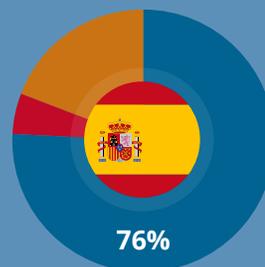
France



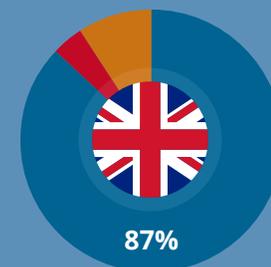
Germany



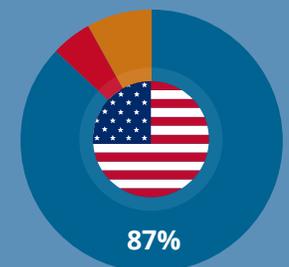
Italy



Spain



United Kingdom



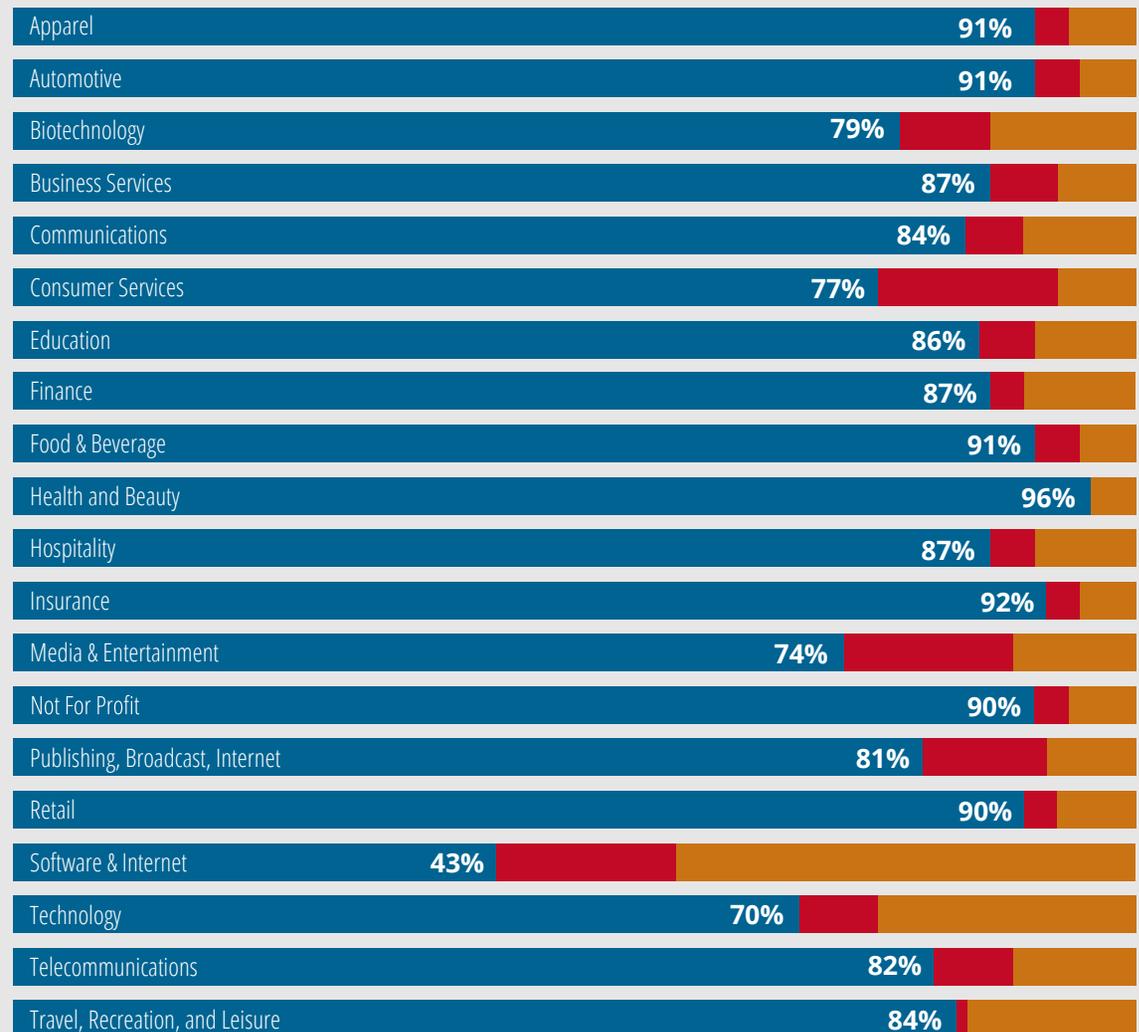
USA

● Inbox ● Spam ● Missing

# Relationship Specialists Perform Best: Inbox Placement by Industry

The industries most dependent on consumer relationships, whether for direct sales (e.g., retailers) or transactional updates (e.g., banks) outperformed others globally. Retailers including apparel and health/beauty marketers posted high inbox placement across the globe, losing less than 10% of their mail to blocking and bulking. Financial services companies, including banks and insurers also reached their customers' inboxes more consistently than others, while publishers, media and entertainment providers trailed other industries.

More granular analysis reveals a far less consistent view of inbox placement performance within industry categories, though. A number of large, global brands were highly successful at maintaining their connections to subscribers throughout the year, exceeding 95% inbox placement and masking erratic performance within their sectors.



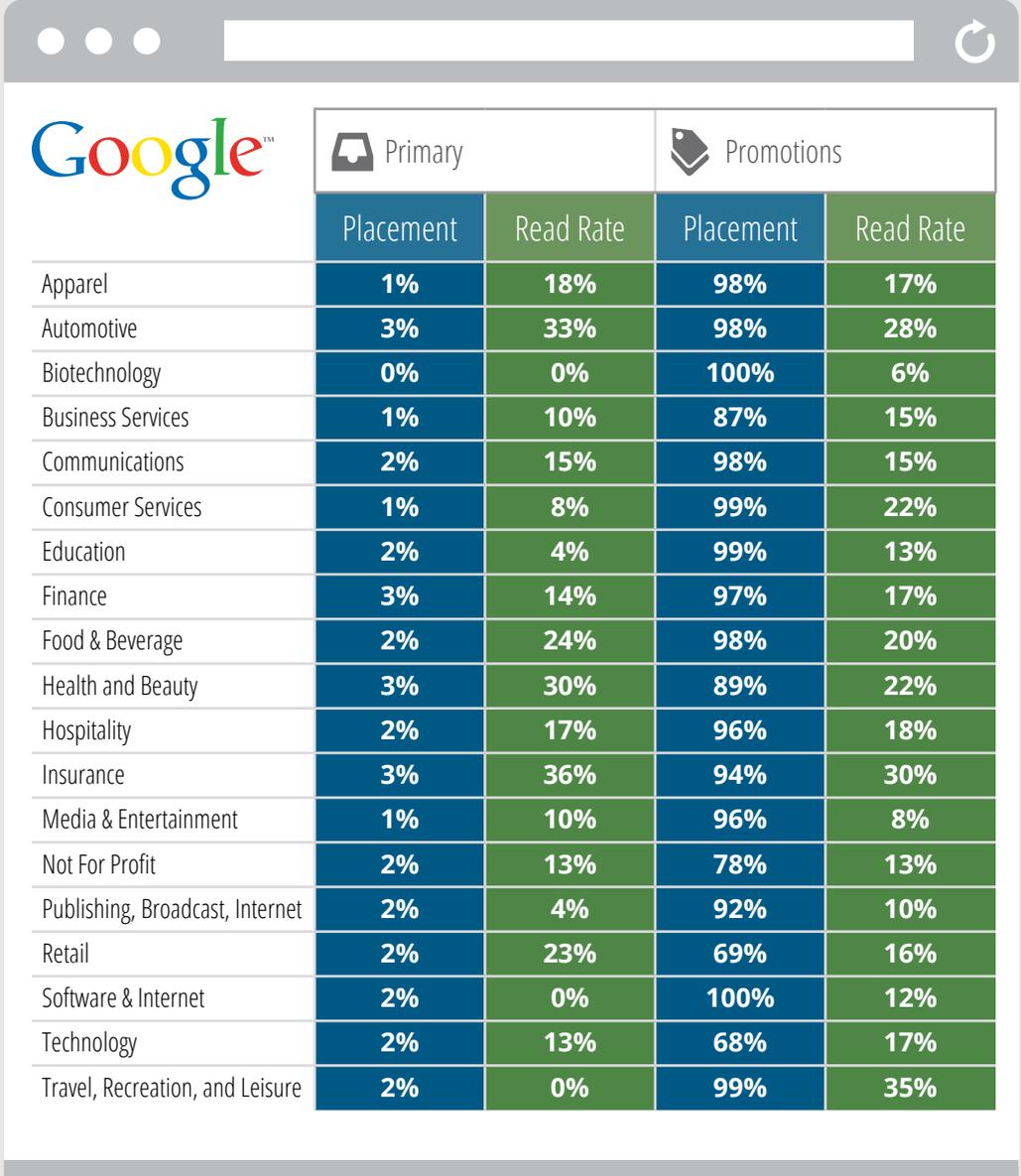
# The Shopping Folder: Inbox Placement and the Gmail Promotions Tab by Industry

Senders had the easiest time hitting their marks when their target was a Gmail box - but only when their messages were routed to the Promotions tab.

Doomsayers foresaw the decline of email marketing in last summer's widespread introduction of the tabbed Gmail inbox, but a year later it appears to be a net gain for commercial senders. Read rates for messages in the Promotions tab have approached 20% in 2014, and inbox placement rates there are among the highest for any large mailbox provider's. Senders that followed Google's suggestion not to ask subscribers to redirect promotional messages into their Primary tabs have been collectively successful at reaching and engaging their audiences, but contrarians have not.

Campaigns meant to convince users to override placement in the Promotions tab failed almost universally, which may have been unexpectedly lucky for their senders: Brands delivering messages to the Primary tab saw much more mail diverted to the spam folder. Gmail warned that commercial mail in the Primary tab would be held to a higher standard, kicked into the spam folder if subscriber behavior didn't clearly indicate it was wanted. That appears to be exactly what happened.

The inbox placement disparity within Gmail's tabs offers a lesson for marketers and for marketing pundits: Consumers like email marketing. Placing commercial messages a click away from the primary tab didn't discourage engagement; instead it created the equivalent of a shopping folder, where consumers actively searched for content they wanted. They ignored commercial messages, though, when they mingled with personal mail; a signal to Gmail that the messages were unwelcome.



Google	Primary		Promotions	
	Placement	Read Rate	Placement	Read Rate
Apparel	1%	18%	98%	17%
Automotive	3%	33%	98%	28%
Biotechnology	0%	0%	100%	6%
Business Services	1%	10%	87%	15%
Communications	2%	15%	98%	15%
Consumer Services	1%	8%	99%	22%
Education	2%	4%	99%	13%
Finance	3%	14%	97%	17%
Food & Beverage	2%	24%	98%	20%
Health and Beauty	3%	30%	89%	22%
Hospitality	2%	17%	96%	18%
Insurance	3%	36%	94%	30%
Media & Entertainment	1%	10%	96%	8%
Not For Profit	2%	13%	78%	13%
Publishing, Broadcast, Internet	2%	4%	92%	10%
Retail	2%	23%	69%	16%
Software & Internet	2%	0%	100%	12%
Technology	2%	13%	68%	17%
Travel, Recreation, and Leisure	2%	0%	99%	35%

# Accelerating Evolution: The Future of Inbox Placement

Defining, measuring, and managing inbox placement is changing fast as consumers' email experience shifts and fractures at a dizzying rate. A recent search of the iTunes store for email apps produced more than 16 million results. Microsoft announced significant changes in its latest update to Sweep, its email productivity toolset. Gmail unveiled Grid View, a Pinterest-style inbox for promotional email, and opened the door to further innovation and customization by releasing a new API for email developers. These influences will only accelerate the evolution of inbox placement; in fact their effects are already visible in this year's report:

## 1 Defining placement in the new inbox:

The compartmentalized inbox introduced by Gmail is already becoming part of other mailbox products, which has complicated the conventional, binary view of inbox placement. Instead of simply being in or out (spam), messages now qualify as inbox-placed regardless of whether they are delivered to the Primary tab or Promotions (or Social, Updates, Forums, etc.).

## 2 Applying new measurement approaches:

Large mailbox providers' increasing emphasis on subscriber engagement as a component of inbox placement is complicating measurement because conventional seed-based assessments can't account for the influence of real users' behavior (see sidebar). One-dimensional views of inbox placement are already inaccurate.

## 3 Rethinking management tactics:

As recently as last year, evaluating sending best practices and following a single set of guidelines was an effective approach to ensuring inbox placement across most mailbox providers. Today their decision making has become more unique and complex, driving senders to adjust email marketing programs for individual providers and even for subscriber segments based on levels of activity, behaviors that indicate secondary accounts, and signals of declining engagement.

### Seeds + Consumer Data: Multidimensional Inbox Placement Analysis

The addition of behavioral data from real subscribers has added a critical dimension to inbox placement analysis, but scalability and nonstandardized preferences limit consumer data's ability to replace conventional seed-based analyses. Email's rapid evolution has necessitated a multidimensional approach to accurately measure inbox placement.

**Defining seed data:** Information captured from high volumes of monitored email accounts (seeds) controlled by senders to sample mailbox providers' placement decisions irrespective of user-initiated or engagement-based filtering. For new programs with little or no history of subscriber interaction, seeds can provide an accurate assessment of inbox placement.

**Defining consumer data:** Information captured from monitored email accounts controlled by real subscribers to sample user-initiated and engagement-based filtering decisions by mailbox providers. Consumer data can uncover behavior-based factors and thresholds that influence inbox placement at large mailbox providers, and can't be identified by non-interactive seeds.



## Methodology

Return Path conducted this study using a representative sample of more than 492 million commercial email messages sent with permission to consumers around the world between May 2013 and April 2014. Global and regional statistics are based on performance across more than 150 mailbox providers in North America, South America, Europe, and Asia-Pacific regions; country- and industry-specific statistics are based on a subset of senders whose location and industry classifications are identifiable.

## About Return Path

We analyze the world's largest collection of email data to show marketers how to stay connected to their audiences, strengthen their customer engagement, and protect their brands from fraud. Our solutions help mailbox providers around the world deliver great user experiences and build trust in email by ensuring that wanted messages reach the inbox while spam and abuse don't. Consumers use Return Path technology to manage their inboxes and make email work better for them.

---

## Contact Us

### **USA (Corporate Headquarters)**

[rpinfo@returnpath.com](mailto:rpinfo@returnpath.com)

### **Brazil**

[rpinfo-brazil@returnpath.com](mailto:rpinfo-brazil@returnpath.com)

### **France**

[rpinfo-france@returnpath.com](mailto:rpinfo-france@returnpath.com)

### **United Kingdom**

[rpinfo-uk@returnpath.com](mailto:rpinfo-uk@returnpath.com)

### **Australia**

[rpinfo-australia@returnpath.com](mailto:rpinfo-australia@returnpath.com)

### **Canada**

[rpinfo-canada@returnpath.com](mailto:rpinfo-canada@returnpath.com)

### **Germany**

[rpinfo-germany@returnpath.com](mailto:rpinfo-germany@returnpath.com)

[returnpath.com](http://returnpath.com)



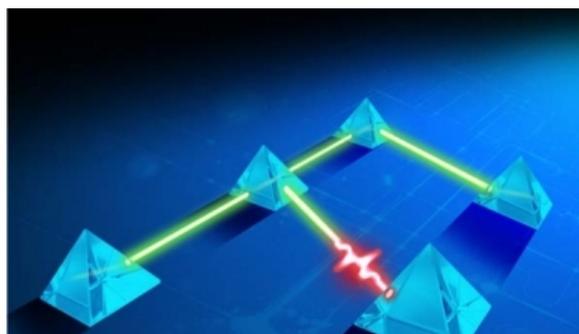
# Why Do So Many Emails Go Undelivered?

Jonathon Mahon | Windows IT Pro

Dec 22, 2014

SHARE Tweet +1 Recommend < 13

COMMENTS 0



Believe it or not, delivering emails isn't as easy as simply clicking the "send" button. In fact, according to research from Return Path, more than 20 percent of emails actually go undelivered. This staggering number is an alarming concern for anyone who is reliant on

email performance—both senders and receivers. In fact, the issue of email deliverability has been a problem for at least a decade, and it will likely continue to remain a concern for some time.

If your email strategy is focused on sending emails only to recipients who grant permission to receive your messages, then delivery challenges will be minimized. However, with mail servers and filters that can often be fickle in their processing, even solicited emails to willing subscribers can be turned away before reaching their intended inboxes.

Here are some factors that prevent an email's delivery:

## ISP-Blocked Emails

The most common form of ISP-blocked emails is for incoming mail. Many larger ISPs maintain internal blacklists of IP addresses that they've chosen to deny from communicating with their servers. This can be caused by customer complaints about too much traffic from particular sources and can lead to ISPs blocking IP ranges without any notification. In an event that is much less common, your ISP may even block your outgoing email traffic to certain ISPs.

## Content Filters

There are a few different types of content filters that may result in emails not reaching their intended destinations. ISPs are often supported by anti-spam companies to help them to filter out distributed content that appears unsolicited based on either the content of the message or its source. Other times, ISPs will employ content filters that are created or adapted internally to scan for a variety of patterns they've associated with spam email, such as inserting spaces or punctuation within words that may normally trigger a red flag. There are also user content filters provided by almost every email client to help users filter certain words, phrases, or even domain addresses into their spam/junk mail folders.

## Message Bounces

An email message may also be bounced back to the sender. A "soft bounce" is a temporary

## SendGrid Resources

- [The State of Today's Email](#)
- [How to Build a Strong Email Call to Action](#)
- [Improving Deliverability of Business-Critical Email](#)
- [Learn The ABCs of ISPs](#)
- [How to Authentically Grow Your Email List](#)
- [The Email Deliverability Guide](#)
- [The Ultimate Email Infrastructure Guide](#)
- [Leveraging Transactional Email for Success](#)
- [Integrating Transactional & Marketing Emails](#)
- [Tips and Tricks to Stay Out of the Spam Folder](#)
- [Build vs Buy: Understanding Email Infrastructure in the Cloud](#)

## Videos

[Click Here to View More Videos](#)

failure to send the email, meaning it wasn't delivered but can try to do so again in the future. This may be caused by the recipient's mailbox being full or their server being unresponsive. A "hard bounce" means that the email has been deemed permanently undeliverable. The cause of a hard message bounce could be that the recipient's email address is invalid or that a remote server is blocking your own server.

\*\*\*\*\*

Before you can optimize delivery, you must understand the common causes of deliverability failure. We hope this post provided a good starting point.

[SHARE](#)
[Tweet](#)
[g+1](#)
[Recommend](#) 13

Please [Log In](#) or [Register](#) to post comments.

### Related Articles

[Email Delivery Toolkit](#)

[Email Like a Person, Not Like a Robot](#)

[Why Do So Many Emails Go Undelivered?](#)

[5 Email Questions with SendGrid's Carly Brantz, Director of Revenue Marketing](#)

[5 Email Questions with SendGrid's Carly Brantz, Director of Revenue Marketing](#)

## Webcasts

[Click Here to View More Webinars](#)

## Email Delivery Toolkit Tweets

Tweets

Follow

 **braintree\_dev** @braintree\_dev 31 Jul

So excited to have @twilio, @SendGrid, @TwitterDev & @pusher as partners at #BattleHack NYC next weekend!

Retweeted by SendGrid

Expand

 **SendGrid** @SendGrid 31 Jul

#Emailmarketing is back on the strategic map! Why it's ideal for creatively engaging with your audience: [send.gd/1JDXSBP](http://send.gd/1JDXSBP)

Expand

 **SendGrid** @SendGrid 31 Jul

We love partnering with @braintree\_dev! #BattleHack NYC is around the corner - join us for prizes and epic battles: [bit.ly/BHnyc](http://bit.ly/BHnyc)

Show Summary

 **SendGrid** @SendGrid 30 Jul

Have #marketers lost the human touch? We hope not, because your customers will surely notice: [send.gd/1JDYmYG](http://send.gd/1JDYmYG)

 **SendGrid Labs** @SendGridLabs 30 Jul

Tweet to @SendGrid



CUSTOMER  
**OBSESSION**  
Empowering Meaningful Relationships

# "Not on the List:" Staying in the inbox and off the blacklist

Speakers:  
Spencer Kollas  
Troy Smith

# About Us

## TROY SMITH

- Client Services Director Senior
- 15 years industry experience
- Director at Experian CheetahMail for 5 years
- Worked on both client and vendors side
- Works with clients across verticals to implement best practices
- Helping clients maintain and enrich customer relationships through multi-channel strategies
- Client Services champion on Deliverability initiatives



# About Us

## SPENCER KOLLAS

- Director, Global Delivery Services
- 8 years email industry experience
- Worked on both client and vendors side
- Create customized programs to help client achieve inbox delivery
- Active member in numerous industry organizations
- Twitter: @SpencerKollas
- Blogs: <http://www.deliverability.com>
- Columnist:  
<http://www.imediaconnection.com>



# Agenda

- Brief History of Deliverability
- Blacklist & Blocklists: What Do I Need to Know?
- Rise of Engagement Filtering
- The NEW Inbox
- Top 5 Stumbling Blocks

# Deliverability: Then & Now



# Deliverability: Then & Now

**NOW**

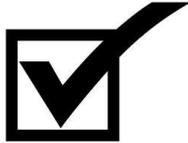
- There was no “This is SPAM” button.
- The decision to deliver was based on volume.
- Inbox providers did not require throttling.
- You could get banished and not know why.
- Reputation was based solely on IP address.
- Data was more about offsetting bad with good or inactive
- Eappend – okay, don’t ask don’t tell

**THEN**

- Reputation is based on IP address and sending domain.
- You must throttle to get delivered...period.
- You could get banished and not know why.
- Where’s our “Like This” button?
- The decision to deliver is based on reputation.
- Data must be managed to remove/avoid out the bad
- Eappend – not so okay, do ask do tell

# The Moving parts of Deliverability

ESP'S RESPONSIBILITY

-  Accreditation
-  Authentication
-  Sending Characteristics

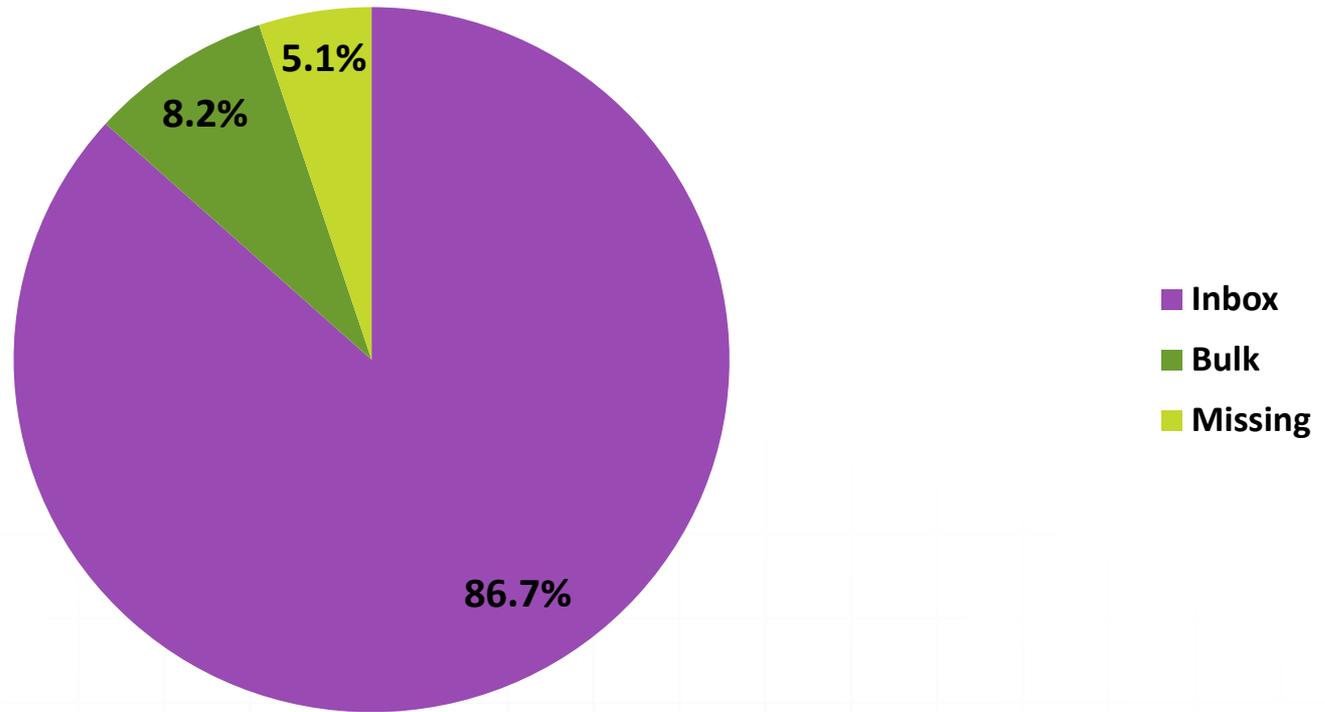


-  Content
-  Sender Reputation
-  List Management

SENDER'S RESPONSIBILITY

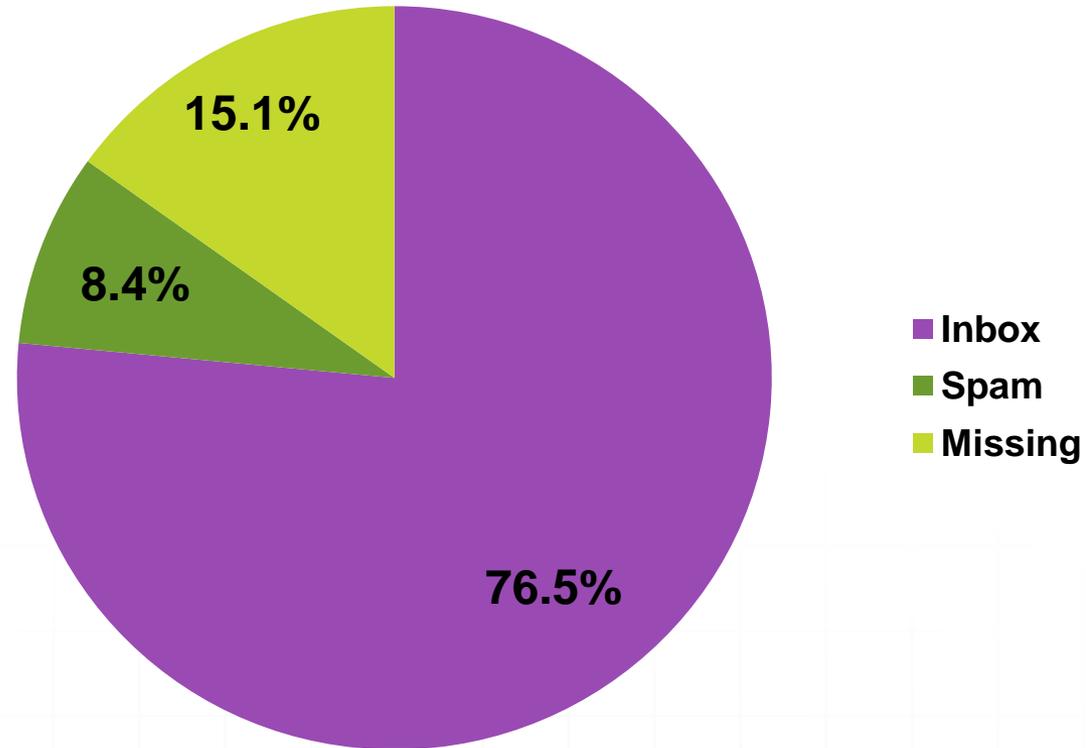
# Worldwide, 1H 2011

## Email Deliverability — Worldwide, 1H 2011



# Worldwide, 2H 2011

## Email Deliverability — Worldwide, 2H 2011



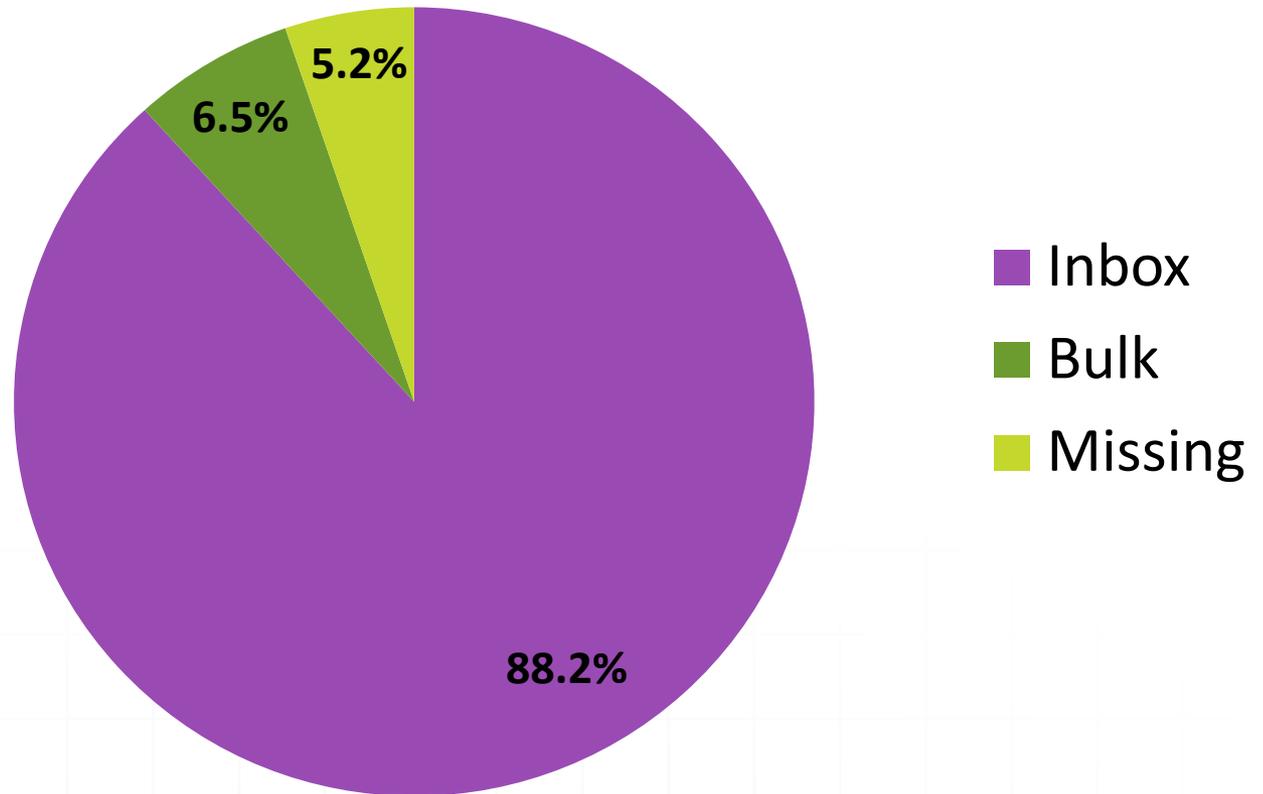
Source: Return Path Global Email Deliverability Benchmark Report, 2H 2011

EXPERIAN CHEETAHMAIL

2012 DIGITAL SUMMIT

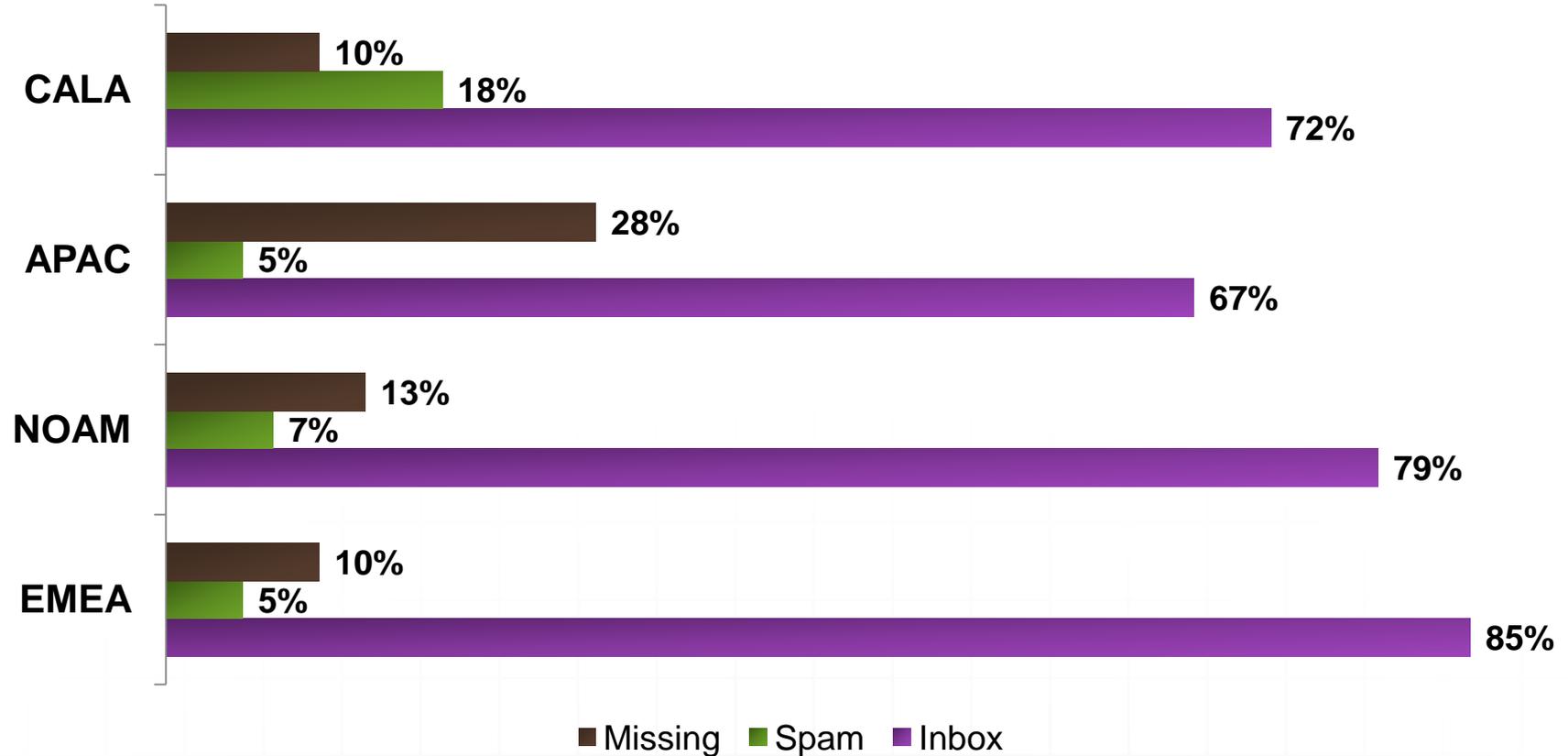
# Worldwide, 1H 2012

## Email Deliverability — Worldwide, 2H 2011



# Global Regions, 2H 2011

## Email Deliverability — Global Regions, 2H 2011



Source: Return Path Global Email Deliverability Benchmark Report, 2H 2011

EXPERIAN CHEETAHMAIL

2012 DIGITAL SUMMIT

# Spam is down, but legitimate email to the inbox is on the rise.

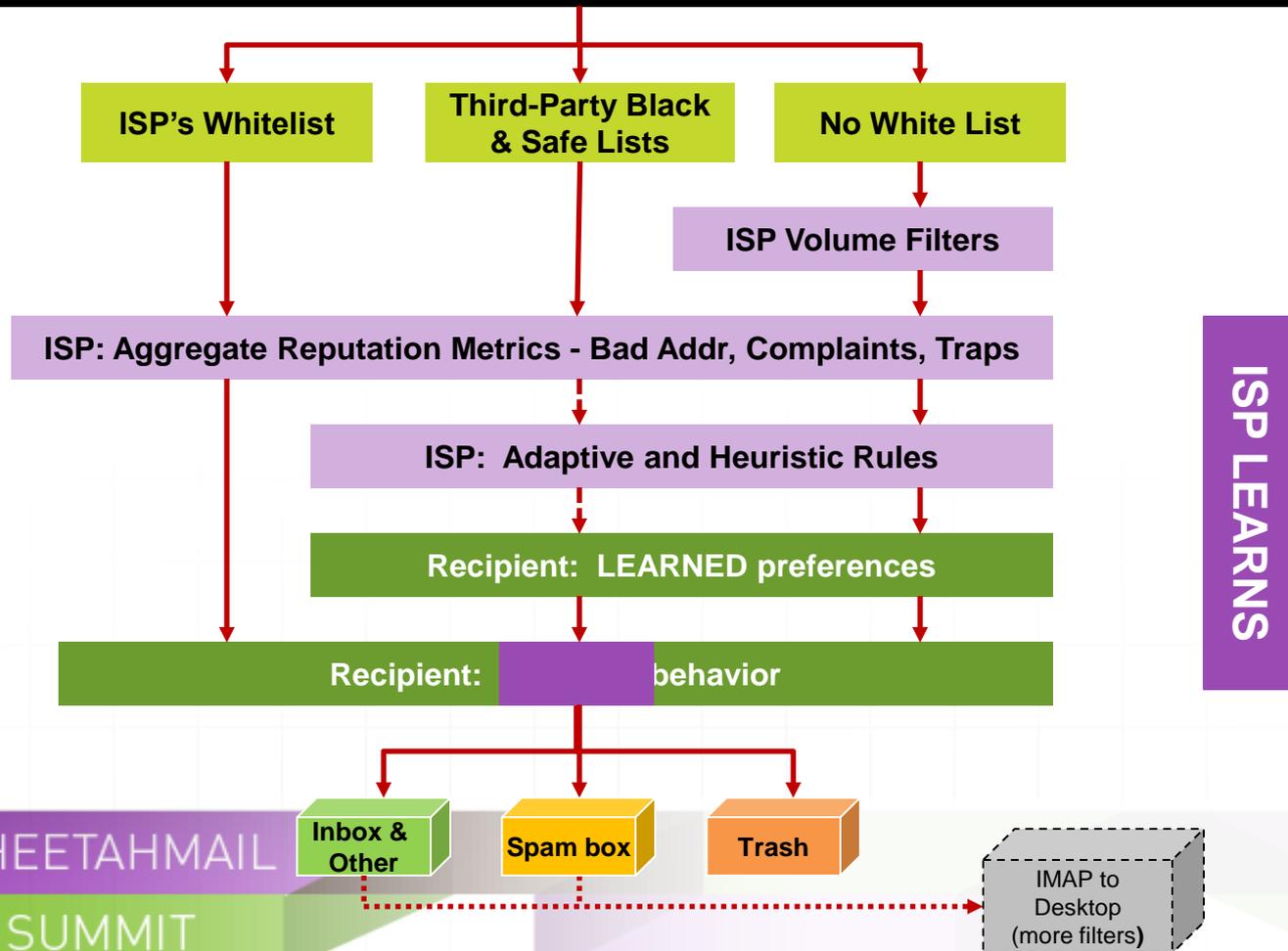
The screenshot shows the Yahoo! Mail interface. The top navigation bar includes 'WHAT'S NEW', 'SPAM (289)', 'CONTACTS', 'SEARCH: jon rardin', 'Strongmail Live Upd...', and 'LinkedIn Network U...'. Below this is a toolbar with 'Compose Message', 'Delete', 'Reply', 'Forward', 'Not Spam', and other icons. The left sidebar shows folders: '3 Bureau CREDIT REPORT', 'Inbox 333', 'Conversations', 'Drafts 3', 'Sent', 'Spam 289', 'Trash 7', and 'Folders' including 'Accucast', 'All Pro Dads-PTA 53', 'BF 1', 'Charter School', 'Cheetah 1', 'Deleted Items', 'Deliverability', 'Fitness', and 'Jobs 6'. The main inbox area displays a list of emails with columns for 'FROM', 'SUBJECT', and 'DATE'. The list is dominated by spam emails, including multiple instances of '60 Minute Deposits', 'CREDIT SCORE ALERT', 'Pure Raspberry Ketone', 'Legal Recall Notice', 'Slim Blast', and 'NEW! NO Computer Required!'. Legitimate emails are also visible, such as 'Jessica <3>', 'Raspberry Ketone', 'Shopper Rewards', and 'Bard Avaulta Mesh Implant Recall'.

FROM	SUBJECT	DATE
60 Minute Deposits	Re: Your \$1,500 Cash Deposit	1:00 PM
CREDIT SCORE ALERT	(2) Recent Changes to Your Credit Score July 10, 2012?	1:08 AM
Pure Raspberry Ketone	Raspberry Ketone: "Miracle Fat Burner in a Bottle" says Dr. Oz. Try it Today!	10:16 AM
60 Minute Deposits	You Prequalify For Up To \$1,500!	7:34 PM
Legal Recall Notice	Get Compensated For Pain Associated With Your Mesh Implant!	1:23 PM
Jessica <3>	View My Pic's.....(NSFW)	6:03 PM
Raspberry Ketone	Raspberry Ketone: "Miracle Fat Burner in a Bottle" says Dr. Oz. Try it Today!	1:40 PM
Shopper Rewards	Activation Required - A New Credit Card for you!	5:35 PM
Legal Recall Notice	Bard Avaulta Mesh Implant Recall - Get Compensation!	9:54 PM
Slim Blast	Get 5 Of Dr. Oz's FAVORITE Weight Loss Ingredients In ONE Miracle Prod...	9:50 AM
★ NEW MAGIC JACK PLUS ★	NEW! ✓ NO Computer Required!	3:04 AM
Credit Card Offer	Activation Required - A New Credit Card for you!	6:01 PM
CREDIT SCORE ALERTS	(2) Recent Changes to Your Credit Score July 1, 2012?	12:09 AM
Slim Blast	Dr. OZ's Favorite Weight Loss Ingredients in ONE Miracle Product!	11:33 PM
ClassesUSASchools	Return To School With A Grant. See If You Qualify!	7:16 PM
Jessica	View My Pic's.....(NSFW)	5:36 AM
Learn a Language	Learn ANY Language in Just TEN Days or Your Money Back!	3:53 AM
60 Minute Deposits	Need Up To \$1,500 In Under 60 Minutes? You Prequalify!	10:07 AM
Green Coffee Extract	Try The New "Magic Weight Loss Cure" According to Dr. Oz! Now 60% Off!	8:03 PM
Raspberry Ketone	Raspberry Ketone: "Miracle Fat Burner in a Bottle" says Dr. Oz. Try it Today!	1:28 PM

# Anatomy of a Typical ISP Process



ISP's Blacklist of Abusive Senders (domains, IPs, networks)/Hard Fail Authentication



# Anti-Spam Blacklists & Public References

## NOTABLE WARNING

**MainSleaze** | *Companies that spam, and ESPs that help them.*

[About this Blog](#) | [What is Mainsleaze Spam?](#) | [The FAQs](#) | [The Bloggers](#)

## MINOR IMPACT



[spamcop.net](http://spamcop.net)

## MAJOR IMPACT

**SPAMHAUS**

THE SPAMHAUS PROJECT

SBL XBL PBL DBL DROP ROKSO WHITELIST

Blocklist Removal Center

[About Spamhaus](#) | [Contacts](#) | [Official Statements](#) | [Sponsors](#)

Spamhaus tracks the Internet's spam senders and spam services, provides dependable realtime anti-spam protection for Internet networks, and works with Law Enforcement to identify and pursue spammers worldwide.

Working to  
Protect Internet  
Networks  
Worldwide

[FAQs](#) | [News Blog](#)



## REPUTATION NETWORK BLACKLIST



USEPROTECT-NETWORK



## NO IMPACT

**\*\*Everyone else\*\***

# Background



- Spamhaus:
  - <http://www.spamhaus.org/organization/index.lasso>
  - The most influential:
    - Extremely powerful automated solution run by volunteers
    - Believes adamantly that all mail is spam unless subscriber has confirmed subscription
  - Increased efforts to block retailers who are mailing old data (12+ months)
    - Inactive data
    - Non-confirmed data
  - Can-spam holds no value
  - Anyone can find out



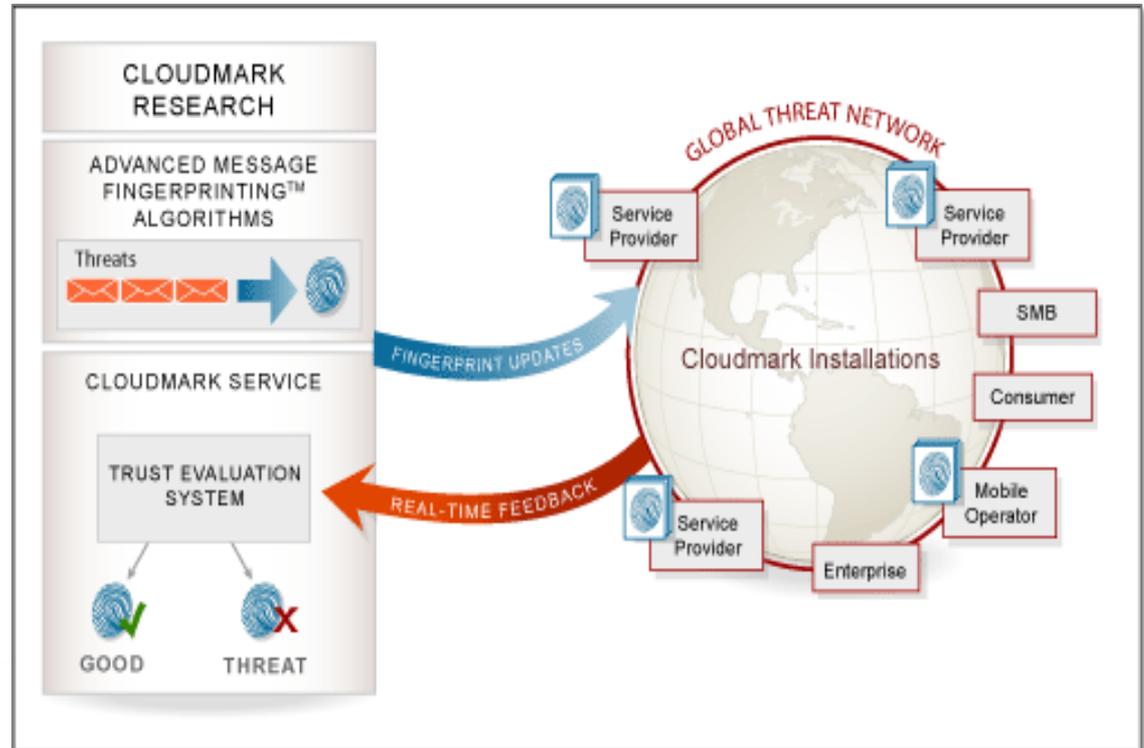
# The Cloudmark Process

## CLOUDMARK STATS:

- Over 100 ISPs
- Protects 750,000,000 inboxes
- 1,000,000 Voters

## FINGERPRINTS REQUIRE:

- 3-40 characteristics
- URLs
- Header information
- Body Content



# Approach Receivers as Ecosystems



# Global Receivers, Filtering Companies & Strategy

## GLOBAL RECEIVERS & FILTERING COMPANIES

**Cloudmark**

**Spamcop**

**Spamhaus**

**Postini  
Barracuda etc**

## DELIVERABILITY STRATEGIES

**List Maintenance**

**Segmentation and  
Monitoring**

**User Engagement**

**Proper Acquisition**

# The Crowded Inbox

Once your  
email is IN...



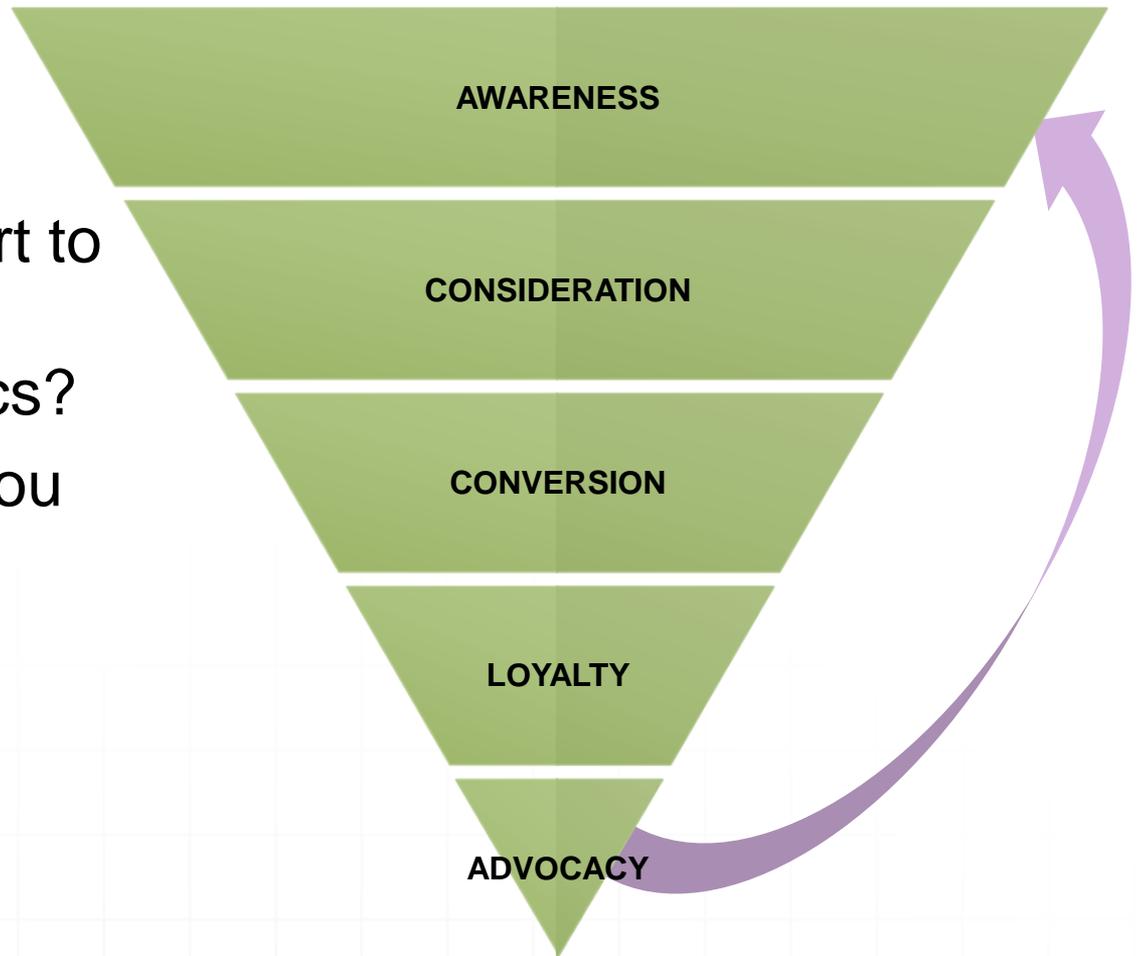
...how do you  
**STAY IN?**

# Subscribers Now Have More Control Over Their Inbox!

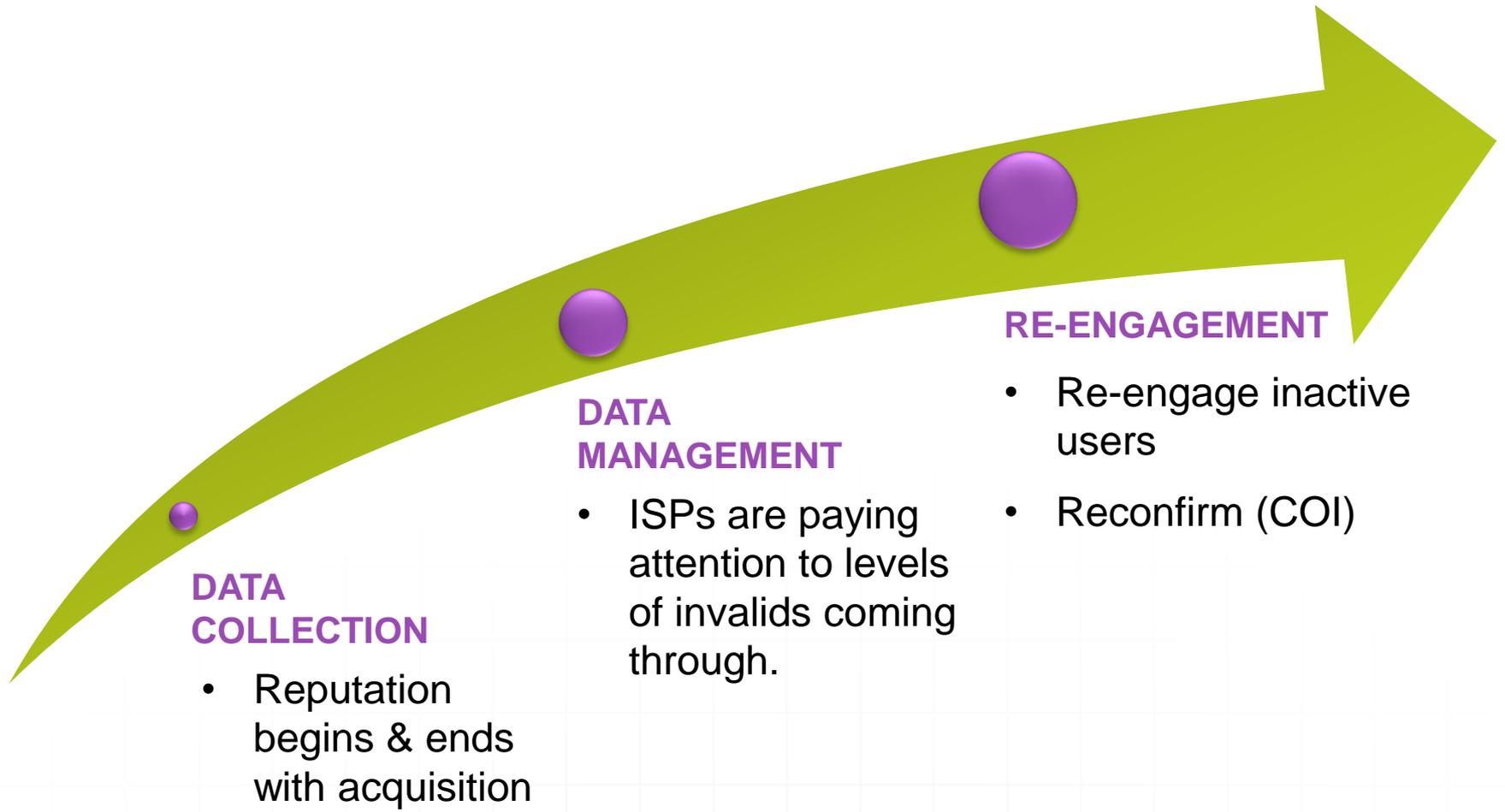
- Hotmail Sweep
- Gmail Priority Inbox
- Gmail Smart Labels
- OtherInbox
- Disposable Email Addresses

# Engagement-based Filtering

- What is it?
- How does it work?
- When will ISPs start to filter based on engagement metrics?
- Is this something you should be tracking already?
- Purchase behavior doesn't play a role



# New Landscape for Deliverability



# Email Deliverability Stumbling Blocks



# 1. You Do Not Have a Permission-based Mailing List

## PROS

- Increase overall possible recipients
- Potentially add new customers

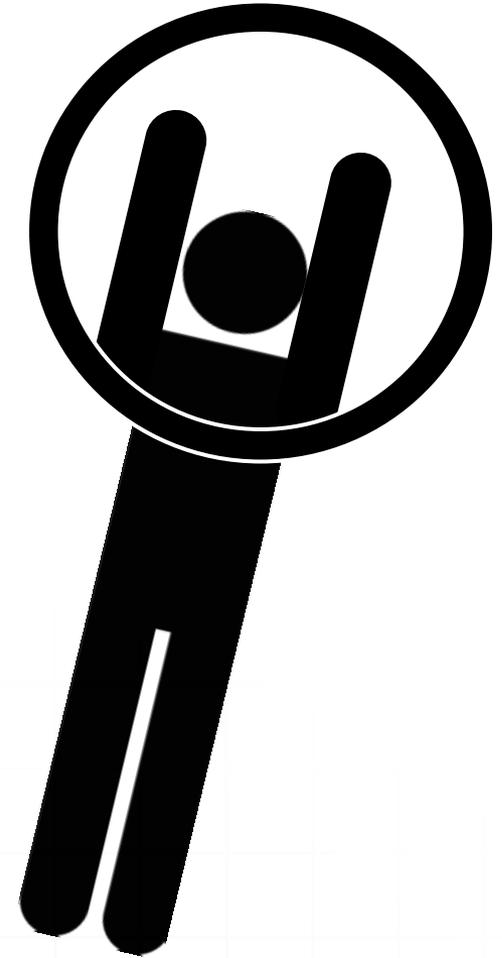
## CONS

- More likely to get marked as SPAM
- High Unknown User Rates
- Low conversion rates
- Potential blacklisting
- Long Term Negative Reputation with ISPs
- Short Term Blocking issues



## 2. Don't Make Potential Subscribers Jump Through Hoops.

- If you want a subscriber to opt-in, avoid making them:
  - Fill out lengthy and irrelevant online forms
  - Click through multiple pages
  - Provide unnecessary information (or information that you don't use in your marketing efforts.)
- The more difficult you make it, the less likely they will be to complete the registration process and subscribe.

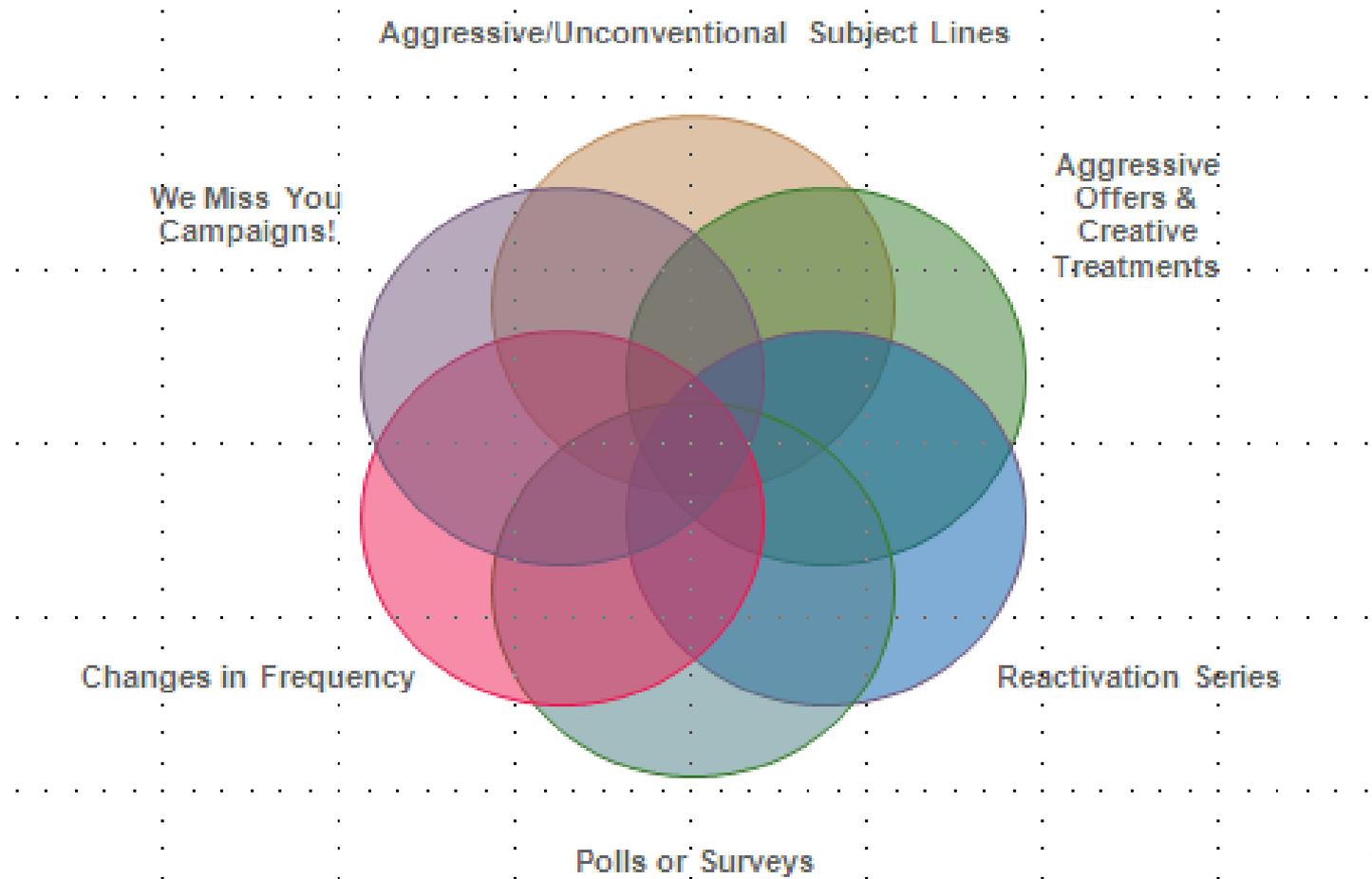


### 3. Too Much Content or Lack of Relevancy.

- Collect profile information that allows you to send relevant and targeted messages that your recipients want to receive.
- Applying basic segmentation and a personalized content strategy across your marketing message allows you to speak directly to your email recipient and create a relevant 1:1 communication strategy.



# 4. No re-engagement plan.





CUSTOMER  
**OBSESSION**  
Empowering Meaningful Relationships

Q&A



# SENDGRID DELIVERABILITY GUIDE V2

Everything You Need to Know About Delivering Email through Your Web Application

# The Most Important Fact about Email:

## DELIVERY IS NEVER GUARANTEED

Email is the backbone of the social web. Can you imagine Facebook without email or any other web application functioning without email? It is the primary—and often the only—channel for communicating with members and customers. Everything from order confirmations to friend requests and privacy updates are sent via email.

Deliverability is a secret crisis facing any business that relies on email communications. Unfortunately, most companies don't think about deliverability until they have a major issue—like when thousands, or in some cases millions, of emails fail to arrive. Businesses falsely assume that an email is delivered if they don't receive a bounce notification. But the reality is very different—according to [ReturnPath's 2013 Email Intelligence report](#), 22% of opt-in emails never make it to the inbox.

What kind of emails are we talking about? Valuable membership confirmations, password resets, shipping notifications, and more. When anticipated messages aren't received, you not only lose revenue, but you also lose your customers' trust.

Consider this quick calculation—if you have a list of one million subscribers and 22% of your emails to those recipients go undelivered, then 220,000 people were left waiting for your email that never arrived. While the impact of this loss is unique to every brand, take a minute to ask yourself: What does losing over 22% of my list mean to me?

In all likelihood, 22% is a lot. So, take the necessary steps to increase the reliability of your email communications now.

### What is Email Deliverability?

Simply put, successful email deliverability is your message arriving in the inbox of the recipient as intended. Email deliverability failure is when your message is either routed to the junk/bulk folder or blocked by an ISP (Internet Service Provider).

So, how do you make sure your email gets delivered? Luckily there are proven techniques to prevent failures and improve your delivery rates for the long-term. This guide offers an overview of the steps most businesses need to take to maximize their email deliverability:

- **BUILD YOUR REPUTATION**
- **SECURE YOUR INFRASTRUCTURE**
- **AUTHENTICATE YOUR MAIL STREAMS**
- **MONITOR YOUR SENDING DATA**
- **SEND GREAT CONTENT**

# Reputation:

## IT WILL OPEN THE INBOX - OR CLOSE IT

The first step in helping ensure email deliverability is reputation. In the world of email, sending reputation refers to a set of specific metrics directly related to your email sending practices. Senders with good reputations get delivered and senders with poor reputations get blocked at the gateway or their messages land in the “junk” folder instead of the inbox.

A strong sending reputation, like a great brand or personal reputation, is built over time. Here are the metrics the ISPs look for when determining sending reputation:

### **RELEVANT, PROPERLY FORMATTED EMAIL:**

Sending quality email that your subscribers want to receive is the basis of a great sending (and brand) reputation. Ensure that your recipients want to receive your email by implementing a clear opt-in during the subscription process and be sure to send relevant and interesting content. Also, make sure your HTML is properly formatted—poorly coded emails get caught in filters or don't render properly.

### **CONSISTENT VOLUME:**

How much email do you send? High-volume senders are always a red flag, especially when volumes are inconsistent. Do you send approximately the same number of emails each week or month, or is your mailing schedule all over the map? Consistent volumes based on subscriber preferences are a key consideration for ISPs.

### **VERY FEW COMPLAINTS:**

Do your subscribers complain or tag your messages as “junk” or “spam”? Even a tiny increase in complaints can cause your email to be blocked by the ISPs. Keeping your complaint rate very low (less than 1% of mail that is sent and accepted by the ISP) is very important.

### **AVOID SPAM TRAPS:**

Sending to even one spam trap or “honey pot” will instantly set back your reputation and cause deliverability problems. When you send to a spam trap (an email address activated by an ISP to catch spammers), it means you're engaging in email address harvesting (an illegal practice) or your list hygiene practices are weak. Either way, ISPs aren't going to deliver your email.

### **LOW BOUNCE RATES:**

A good reputation also means that only a small percentage of your emails “bounce” back or are returned by the ISPs because the account is no longer active (hard bounce) or the mailbox is temporarily full or the recipient is out-of-office (soft bounce). If a lot of your mail is bouncing back, it means your subscribers aren't engaged and you're not keeping up to date with them. It also indicates that your list hygiene practices are not up to industry standards. This makes your email look like spam to an ISP and your email is unlikely to get delivered. Keeping your bounce rate low by implementing procedures to immediately remove email addresses that return “hard” bounces is essential.

### **NO BLACKLIST APPEARANCES:**

Appearing on just one of the leading blacklists is enough to get you blocked by some ISPs. Senders with low complaints, who don't hit spam traps, and who send email consistently generally don't get blacklisted. However, if you do get blacklisted, having a good sending reputation will help convince the blacklist administrator to remove your IPs from their list.

# Reputation:

## IT WILL OPEN THE INBOX - OR CLOSE IT



### BEST PRACTICE TIP

#### HOW TO AVOID SPAM TRAPS

As we mentioned, hitting just one spam trap is a reputation killer. To avoid including a spam trap email in your mailing list, have an industry standard opt-in process, don't rent or buy email lists and keep your list clean.

# Infrastructure:

## THE FOUNDATION OF DELIVERABILITY SUCCESS

Setting up and maintaining infrastructure for high-volume email is complex, challenging, and expensive. It's not as simple as maintaining a corporate email environment, and very different rules and standards apply. You'll either need dedicated staff who understand the ins and outs of email to monitor your email program, or you can turn to an email service provider like SendGrid who can take care of everything for you.

### CAN YOU AFFORD TO HAVE YOUR MESSAGES BLOCKED FOR SEVERAL HOURS OR DAYS? DO YOU KNOW THE CURRENT STATE OF YOUR INFRASTRUCTURE? HERE ARE SOME QUESTIONS TO ASK:

1

#### Are you using a dedicated IP Address?

If you're a high-volume sender who is working with an email provider, make sure you have an IP address dedicated to your mail stream. Ideally, have at least two IPs, one for your transactional email and a second for your marketing/promotional email. Sharing an IP address with other senders means their practices and reputation will have a direct impact on your deliverability—and that's not good for any business. (At SendGrid, a dedicated IP address is provided for all plans [Silver and higher](#).)

2

#### Are your mail servers secured or could a hacker use them for spamming?

Make sure you don't have an open relay or open proxy. Follow industry standard best practices for network and server security. All the best mailing practices don't matter if you don't have control of your environment.

# Infrastructure:

## THE FOUNDATION OF DELIVERABILITY SUCCESS

3

### Are you signed up for ISP Feedback Loops?

And do you have a process for managing complaints? Not only do you need to get signed up for all major ISP feedback loops, but you also need a process for rapidly removing email addresses that log complaints. Continuing to mail to people who have reported your email as spam will result in deliverability failures. (Gmail doesn't have feedback loops, so be sure to implement a List-Unsubscribe header for more insight. Find more information about the [list unsubscribe header here](#).) SendGrid automatically registers all users for all major feedback loops.

4

### Do you have “postmaster” and “abuse” mailboxes set up for all your domains?

If yes, are you monitoring them? Many ISPs require that these mailboxes be set up and working to get access to their feedback loops. These are also common destinations for complaints from ISPs that don't have feedback loops.

5

### Is your sending domain able to receive mail?

Your sending domain needs to be able to receive mail, and it must have a valid MX record. If not, some ISPs will block your email.



## BEST PRACTICE TIP

### RESIST THE TEMPTATION TO MOVE IP ADDRESSES TO RESOLVE DELIVERABILITY PROBLEMS.

Resist the temptation to move IP addresses to resolve deliverability problems. This is a suspicious practice and ISPs treat new IPs with caution. In fact, all IP addresses start with no reputation and must be “warmed up” by your good practices. Start by sending low volumes of email and work your way up to larger volumes. This helps you build a solid reputation and improves your chances of getting high delivery rates. If your mailing practices are poor or infrastructure is not managed properly these problems (and the bad reputation) will follow you to your new IP address. Need help with your infrastructure and deliverability? Just ask. [SendGrid's team of experts](#) is ready to help.

# Authentication:

## SECURE YOUR IDENTITY AND MAKE THE (EMAIL) WORLD SAFER

Authentication is an “ID check” for your mail streams: it validates that the email is actually from you, and not some spammer impersonating you. Authenticating your mail streams does not ensure that your email will be delivered, but it helps ISPs to further differentiate your business from spammers and other illegitimate senders. As fraudulent “phish” emails and other deceptive practices endanger consumers and businesses, authenticating your email is one positive step you can take today to make the [email] world a better place.

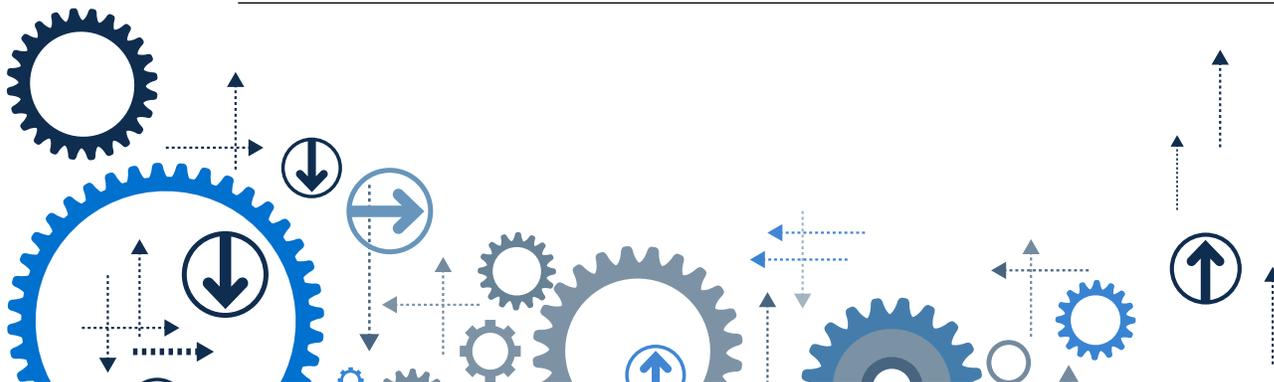
### How Does Authentication Work?

There are two main methods of authentication that you should implement:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)

Here's what you need to do to get started:

- 1 Get informed. You can find detailed information on DKIM and SPF here:  
DKIM: <http://www.dkim.org> SPF: <http://www.openspf.org>
- 2 Take stock of all systems that send your mail and identify all machines that send mail for your company. Next, determine the IP addresses and sending domains used.
- 3 Create your authentication records.
- 4 Publish your authentication records. Work with whoever manages your DNS records to publish the email authentication records you've collected.
- 5 Set up your mail server to sign outbound email with DKIM. DKIM requires that your MTA has the appropriate software implementation to sign all outgoing emails. Learn more at: <http://www.sendmail.com/sm/wp/dkim>
- 6 Test your authentication records. SPF and DKIM provide options to publish your records in “test” mode. This provides the opportunity for testing without risking delivery failures.



# Authentication:

## SECURE YOUR IDENTITY AND MAKE THE (EMAIL) WORLD SAFER

### Domain Reputation

Domain reputation identifies legitimate senders based on their domain name rather than their IP address by using the DKIM authentication protocol. There has been a sharp move towards domain reputation predicated by the move from IPV4 networks to IPV6 networks. While it's not yet common practice to use domain reputation required under IPV6 (though Gmail is already the strongest proponent), the ISPs are starting to use the combination of IP and domain reputation until IPV6 is fully adopted.

The key benefit to domain reputation is reputation portability that enables ISPs to track sender reputation regardless of IP and frees senders to move between email service providers. Domain reputation will also help senders who move to a new IP to not have to warm up. The theory is (and keep in mind this is a theory), if you have a domain that has a good reputation, when you move to a new IP address, recipient ISPs will not require senders to warm up their IP because they will already know what volume to expect due to your domain's reputation.

This also means if you tarnish your domain reputation, it makes it much more difficult to start from scratch with a new domain.

Bottom line: Senders should focus on both domain and IP reputation in order to maximize email deliverability.



### BEST PRACTICE TIP

#### MAKE SURE YOUR DATA COLLECTION PRACTICES ARE SOUND.

Use your welcome message, or even the first three to five messages to ferret out bounces, ill-formed addresses, and even sources with a high likelihood of complaining. With good list hygiene practices and regular data monitoring, you can earn a good reputation and high delivery rates.



# Your Emails:

## FIVE BASICS TO KEEP YOUR REPUTATION INTACT – AND YOUR MEMBERS HAPPY

1

### ASK PERMISSION, HOST A PREFERENCE CENTER

Watch out for email fatigue. Sending too much email to your users can drive high unsubscribe and/or complaint rates. Offer a preference center so users can choose what updates they'd like to receive and how often they would like to receive them.

---

2

### KEEP A CLEAN LIST, AVOID TRAPS

A clean, well-managed subscriber list can be your best asset, whereas “dirty” lists with out-of-date information are a leading cause of deliverability failures and are sure to damage your sending reputation. List hygiene is the process of removing “bad” addresses in a timely manner. Good list hygiene practices are essential to avoiding spam traps and keeping your bounce rates low—key drivers of your reputation. There is no better way to ensure consistent deliverability success than by regularly cleaning your list of hard bounces, unknown users, and other inactive addresses. SendGrid's real-time [Event Webhook](#) is a great start, providing instant information like opens, bounces, and unsubscribe requests for individual subscriber records.

Also, implementing regular reconfirmation/win-back campaigns is a good way to ensure that your lists stay clean. These campaigns help you remove unengaged users so your lists are up to date. The frequency of sending win-back campaigns depends on your business, but at a minimum, you should be sending them yearly, though we recommend sending them quarterly.

---

3

### SEND A WELCOME MESSAGE

Welcome messages are the cornerstone of a well-run email program. When was the last time you signed up for a new online service and didn't receive an immediate message confirming the sign up? Welcome messages (like other transactional emails) are more than confirmations, they're an opportunity to engage with subscribers and to start the relationship off on the right foot.

---

4

### FOLLOW THE LAW

Be sure to comply with the federal CAN-SPAM Act. The CAN-SPAM Act is geared towards marketing email (with transactional email technically being exempt), but we advise that senders follow its regulations regardless of what type of email they send. Here's what you need to do:

- Have a working unsubscribe mechanism in the footer and/or header of all email communications.
- Include your official business street address in the footer of all email communications. This should be your corporate headquarters or another address where official communications are handled. It cannot be a P.O. Box.
- Handle all unsubscribe requests within 10 business days. This means when someone asks to be removed from your list, you must suppress that email address from future mailings within 10 business days. This is the minimum, and ideally the suppression should occur within 24 hours.

*Quick disclaimer: the tips above are not legal advice, you should get professional advice from a lawyer to address any specific concerns around compliance.*

Complying with CAN-SPAM is ultimately the bare minimum when it comes to sending email. We recommend stepping it up a notch and going above and beyond CAN-SPAM by following the other recommendations in this guide.

# Your Emails:

## FIVE BASICS TO KEEP YOUR REPUTATION INTACT – AND YOUR MEMBERS HAPPY



5

### SEND GOOD EMAIL

It sounds obvious, but it's actually harder than it sounds. There is no secret formula to sending email that works. First, make sure you're following the four suggestions outlined above. Second, the content of your emails needs to be relevant, interesting, and aesthetically aligned with your brand. Ask yourself some basic questions before you hit send:

- Have I asked my subscribers what kind of content they want to receive?
- Will my subscribers want to read this email?
- Have I included both an HTML and a plain text version?
- Is my email optimized for mobile?
- Is my email a positive reflection of my brand?
- Overall, am I getting the right message, to the right subscriber, at the right time?



### BEST PRACTICE TIP

#### **DON'T USE NOREPLY@DOMAIN.COM IN YOUR EMAILS.**

Webmail email providers like Yahoo! and Gmail automatically add email addresses that users reply to, to their contacts list. Messages from senders in the contact lists won't be marked as spam in most cases. The best way to start is to allow registered users to reply to emails to confirm their email accounts in addition to providing a confirmation link. Also, letting customers reply directly to your email lets them know that you want to hear from them. Your goal is to stimulate a two-way conversation with your user. Using a "no reply" in your "from" address can elicit a negative response from your customer. So, send your emails from an email address that can be regularly monitored for responses.

## Summary

### KEEP YOUR REPUTATION INTACT--AND YOUR MEMBERS HAPPY



- Email delivery is never guaranteed. Think about how losing 22% of your email affects your bottom line.
- To help your email get delivered you need to be on top of your reputation, make sure your mail streams are authenticated, manage a complex infrastructure, and monitor your sending activity.
- Email deliverability relies on good list hygiene and sending relevant, quality content.

## Get started with SendGrid

Relieve yourself of the cost and complexity of maintaining your own system.

[Learn More](#) ▶

[Read Our Customer Success Stories](#) ▶

[Sign Up](#) ▶

## About SendGrid

**SENDGRID IS EMAIL DELIVERY. SIMPLIFIED.**



If you'd rather focus on growing your business than on email infrastructure, SendGrid is here to help. SendGrid helps you focus on your business without the cost and complexity of owning and maintaining an email infrastructure. We manage all technical details, from scaling the infrastructure, to ISP outreach and reputation monitoring, to whitelist services and real-time analytics. We offer world-class deliverability expertise to make sure your emails get delivered and handle ISP monitoring, DKIM, domain keys, SPF, feedback loops, whitelabeling, link customization, and more.

Getting started with SendGrid has never been easier. [Sign up here.](#)

# Learn

The ABCs of ISPs



**Email deliverability is critical to the success of any email program.**

**One of the best ways to ensure your email gets delivered is by complying with guidelines set by Internet service providers (ISPs—also called mailbox providers) like Gmail, Yahoo!, and Outlook.**





# What's Inside

As email continues to evolve, it's important to follow the best practices that will help your email reach the inbox. At SendGrid, we communicate with ISPs to help us stay on top of issues that affect our clients' deliverability. In this guide, you'll learn how to get delivered at the major Internet service providers.



- 01.** Overview
- 02.** Email Deliverability Strategies
- 03.** Email Deliverability Tools
- 04.** Email Deliverability Tactics
- 05.** Email Deliverability Results

# Overview

## The Email Delivery Landscape is Ever Changing

As the email industry has grown more sophisticated, it's become congested by legitimate mailers who use email to communicate with their customers, but also by spammers who continue to invent ways to thwart mailbox providers.

According to *Mashable*, in 2012, over 144 billion emails were sent worldwide every day and 65% of those were spam (**figure 1**).<sup>1</sup> Mailbox providers are doing an amazing job at keeping spam out, but with a problem this big, many times legitimate messages fail to get through. This is why it's important to understand the factors that affect delivery, and implement the best practices that can help mailbox providers identify good mail and keep out the bad. The ISPs' goal is to protect consumer inboxes from malicious email, not to stop your email from getting through.

### As an aside...

*Mailbox providers include ISPs and spam filtering solutions. We will use these terms interchangeably within this guide to include the entire group.*



**FIGURE 1** Email statistics from Mashable

## The True Meaning of Undelivered Email Today

22% of commercial email never makes it to the inbox.<sup>2</sup> **Transactional email** is especially vulnerable—the 2012 Websense Threat Report revealed that 92% of spam contains a web link.<sup>3</sup> Transactional email tends to achieve higher deliverability, because it's more desired by customers. Unfortunately, it still falls victim to the same email traps and filters as commercial email, and the effect can be detrimental to any brand.

If email drives any of your revenue, you can quantify the impact of email not reaching the inbox. Even with softer goals like new user acquisition or engagement, you're missing out on a huge segment of potential users and customers.

### According to our survey:

- » **80.5%** rely on email for signups and subscriptions
- » **76.5%** for password recovery and account changes
- » **49.8%** for order and shipping confirmations
- » **28%** use for friend/follower requests and confirmations

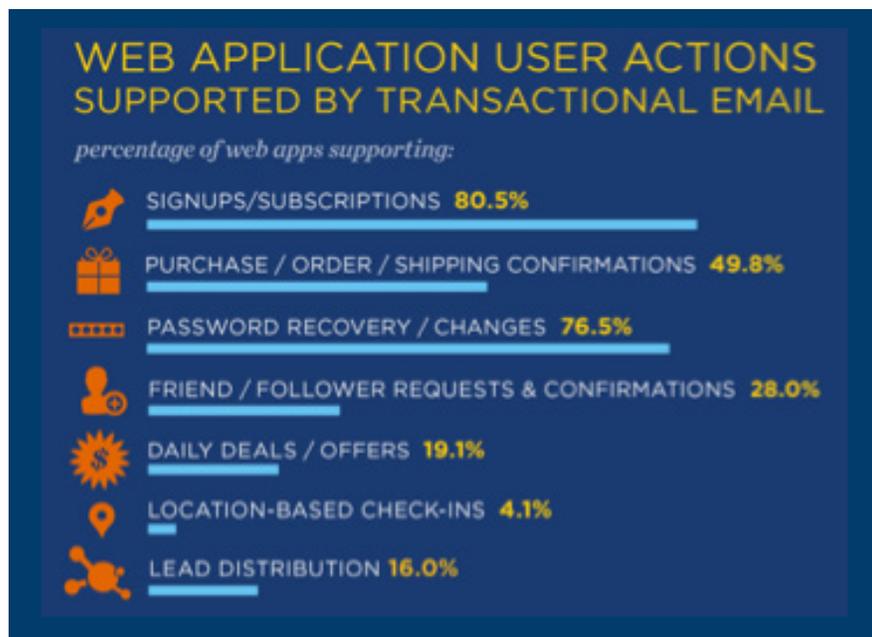


FIGURE 2

SendGrid: The Evolution of Transactional Email



For many companies, especially web apps, growing your user base is imperative for driving business and attracting more investors. Paying close attention and understanding how mailbox providers view your email is essential for the success of your email program.



# Email Deliverability Strategies

## Getting Delivered Starts with Your Reputation

**Email deliverability** is the total number of emails successfully delivered to the ISPs divided by the total number of emails sent. The higher your deliverability rate, the more emails make it to the inbox.

Email deliverability is influenced by a lot of factors, including signing your mail, keeping clean lists, sending wanted content, having a good sending reputation, and much more. Your sending reputation is how ISPs identify you as a legitimate sender. Every time you deploy an email campaign, you are providing them with valuable data that says whether or not you follow proper sending practices. There are two types of reputation—IP Reputation and Domain Reputation.

---

### » IP Reputation

Email is sent from IP addresses, which serve as unique identifiers of email streams. Some companies send from a shared IP, which means multiple companies use the same IP address to deploy their email. Senders with more volume usually opt to send from a dedicated IP address that belongs only to their organization. By using a dedicated IP, you can better control your IP reputation because you're not impacted by other senders' bad practices. At SendGrid, a dedicated IP address is offered with **all packages Silver and higher**.

### » Domain Reputation

Your domain reputation is based on your sending *domain* instead of your IP address. This means that your *brand* takes precedence when it comes to ISP filtering decisions.

There has been a sharp move towards domain reputation predicated by the move from IPV4 networks to IPV6 networks. While it's not yet common practice to use domain reputation, required under IPV6 (though Gmail is already the strongest proponent), the ISPs are starting to use the combination of IP and domain reputation until IPV6 is fully adopted.

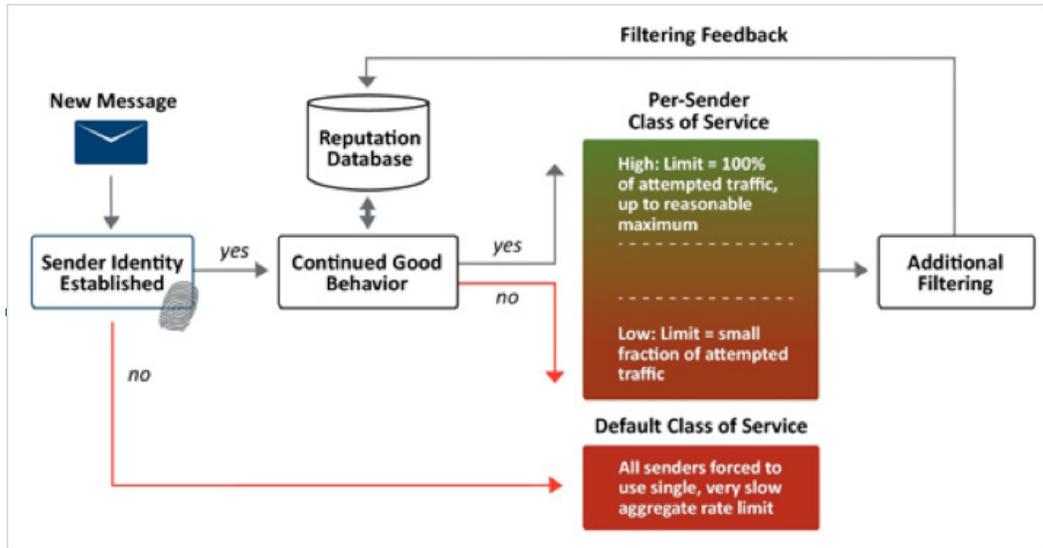
*(Continued on next page)*

The idea of “portable reputation” is very appealing to senders who want the flexibility to add new IPs, move IPs, or change email service providers (ESPs) without losing the good reputation they’ve already built from their sending activity. Domain reputation also eliminates the need to warm up new IPs since ISPs use the reputation of the entire domain as their filtering metric. (With IP reputation, you lose all reputation history and data when you change IPs or ESPs.) As a result, new protocols have been developed to help facilitate domain reputation as the next frontier for filtering.

Most importantly, with domain reputation, you can’t change an IP address to fix reputation problems. Email sending mistakes can now affect your domain reputation and your brand in a bigger way than it ever has before. This is why it’s so important to have good sending practices.

## » Authentication

To help safeguard your reputation, senders should start with email authentication. Authentication helps ISPs identify which IPs and domains rightfully belong to you. Here’s how it works (**figure 3**).



**FIGURE 3** How email authentication works courtesy of Cloudmark, a provider of tools and services that protect against messaging abuse.<sup>4</sup>



There are several authentication methodologies the **Messaging Anti-Abuse Working Group** suggests you implement:

*Senders should incorporate as many authentication standards and technologies as their systems can support for each of their messaging streams: Transactional, Marketing, and Corporate. These standards can range from mechanisms that help identify mailers by linking IPs to domains (Sender Policy Framework, known as SPF, and Sender ID) to more complicated cryptographic technologies like Domain Keys Identified Mail (DKIM).<sup>5</sup>*

DKIM and SPF are imperative in tracking reputation, but **Domain-Based Message Authentication, Reporting, & Conformance** (DMARC) is the next evolution of email authentication. DMARC allows email senders to specify how ISPs should treat emails that have not been authenticated using SPF or DKIM. Senders can opt to send those emails to the junk folder or block them all together. ISPs can then better identify spammers and prevent malicious email from invading consumer inboxes, while minimizing false positives and providing better authentication reporting for greater transparency in the marketplace. To learn more about DMARC compliance, [read our blog post on the topic here](#).



### Recommended Reading

Learn more about how to authenticate your email and the different authentication methods by [downloading the SendGrid Email Infrastructure Guide](#).



## Consistent Delivery = Sending + Engagement

Mailbox providers use a series of reputation and engagement metrics to determine email deliverability. By understanding all of these factors, you can better influence the outcome of your email program.

---

### Reputation Metrics

Each ISP makes filtering decisions based on a series of reputation metrics. While thresholds vary by ISP, it's important to know that each time you deploy messages to your email list, your reputation is impacted. Three key factors that will affect your reputation include:

#### » Spam Complaint Rate

This is the percentage of subscribers who have reported your email as spam. A high complaint rate is the number one factor used by ISPs to determine whether or not to deliver your email messages. If too many people are flagging your mail as spam, ISPs will take action to block your messages.

#### » Unknown Users

This is the number of emails on your list that are non-existent email addresses, which bounce back messages. Common reasons for this include misspelled emails and full inboxes. If an email address has bounced more than once, you should remove the address from your list.

#### » Spam Traps

This is the number of messages sent to email addresses set up specifically to catch spammers. Spam traps (or “honey pots”) often appear if you have poor email acquisition practices or if your email list is too old. ISPs set up specific accounts or often reclaim accounts with no activity and monitor the messages that are sent to those inboxes. Since these addresses will never open or click on your messages, it's important to practice good list hygiene and proactively remove non-engaging addresses.

## Engagement Metrics

ISPs consistently enhance filtering algorithms by adding metrics to identify legitimate email. There is a new focus on email engagement that evaluates whether your users are actually interacting with your messages.

Many ISPs now look at customer activity to determine whether or not to deliver email. ISPs often use custom algorithms to measure engagement, but common metrics may include the following:

### » Open Rate

This measures how many subscribers “looked at” your email. However, the only way this metric is counted is if the images included in the message are downloaded. However, many subscribers have images automatically turned off, so despite viewing your message, they will not be counted in the open rate.

### » Clicks

This is the number of subscribers who clicked on one or more links in your email message.

### » TiNs Data

This is collected when users actively click a button that says “This is Not Spam.” It shows that users want your email and will help improve your reputation (**figure 4**).



**FIGURE 4** Courtesy of [www.webdevelopersnotes.com](http://www.webdevelopersnotes.com)



### »» **Saving to Folders**

Retaining email by moving it from the inbox to another primary folder is a sign of engagement. Negative engagement would be mass deleting or a user taking no action.

### »» **Panel Data**

A panel of users who determine whether email messages have been correctly marked as spam based on criteria specified by the email providers.

### »» **Trusted Reporter Data**

Compiled accounts that have proven to be real users who demonstrate normal behavior when interacting with their email messages.

### »» **Inactive Accounts**

Mailboxes that do not have regular activity.

### »» **Recent Interaction**

The number of users who have interacted within a specific period of time demonstrates the value of your offer.<sup>6</sup>



#### **Engagement Tip: Get Rid of the “No Reply.”**

Let customers reply directly to your email. Your goal is to stimulate a two-way conversation with your user. Using “no reply” in your from address can elicit a negative response from your customer. So, send your emails from an email address that can be regularly monitored for responses.

To do that, use the [SendGrid Parse Webhook](#) to extract data from your emails and send responsive emails to your customers. For example, offer your users a 15% discount if they reply to your email. When they respond, an automatic message can be sent with a discount code.



# Email Deliverability Tools

## Your Reputation Is Always In Your Control

The anti-abuse community is fairly small, and they communicate regularly. So, word will get around very quickly if you make an effort to do the right thing. On the flip side, bad deeds will not go unpunished. Your reputation is always in your control, but you first have to understand where you stand. Here are several resources for checking your sending reputation:

---

### »» [SenderScore.org](#)

Like a credit score, a Sender Score is a measure of your reputation. Scores are calculated from 0 to 100. The higher your score, the better your reputation and the higher your email deliverability rate. Numbers are calculated on a rolling 30-day average and illustrate where your IP address ranks against other IP addresses. This service is provided by Return Path.

### »» [Senderbase.org](#)

Senderbase is a product of Cisco and provides you with the tools to check your reputation by ranking you as Good, Neutral, or Poor. Good means there is little or no threat activity. Neutral means your IP address or domain is within acceptable parameters, but may still be filtered or blocked. Poor means there is a problematic level of threat activity and you are likely to be filtered or blocked.

### »» [BarracudaCentral](#)

Barracuda Networks provides both an IP and domain reputation lookup via their Barracuda Reputation System; a real-time database of IP addresses with “poor” or “good” reputations.

### »» [TrustedSource](#)

TrustedSource is a site very similar to [senderbase.org](#), but run by McAfee. It provides information on both your domain’s email and web reputations as well as affiliations, domain name system (DNS), and mail server information. It also provides details on the history, activation, and associations of your domain.



### » ReputationAuthority

WatchGuard’s ReputationAuthority helps protect business and government organizations from unwanted email and web traffic that contain spam, malware, spyware, malicious code, and phishing attacks. You can look up your IP address or domain, receive a reputation score from 0-100, and get the percentage of emails that were good versus bad (figure 5).

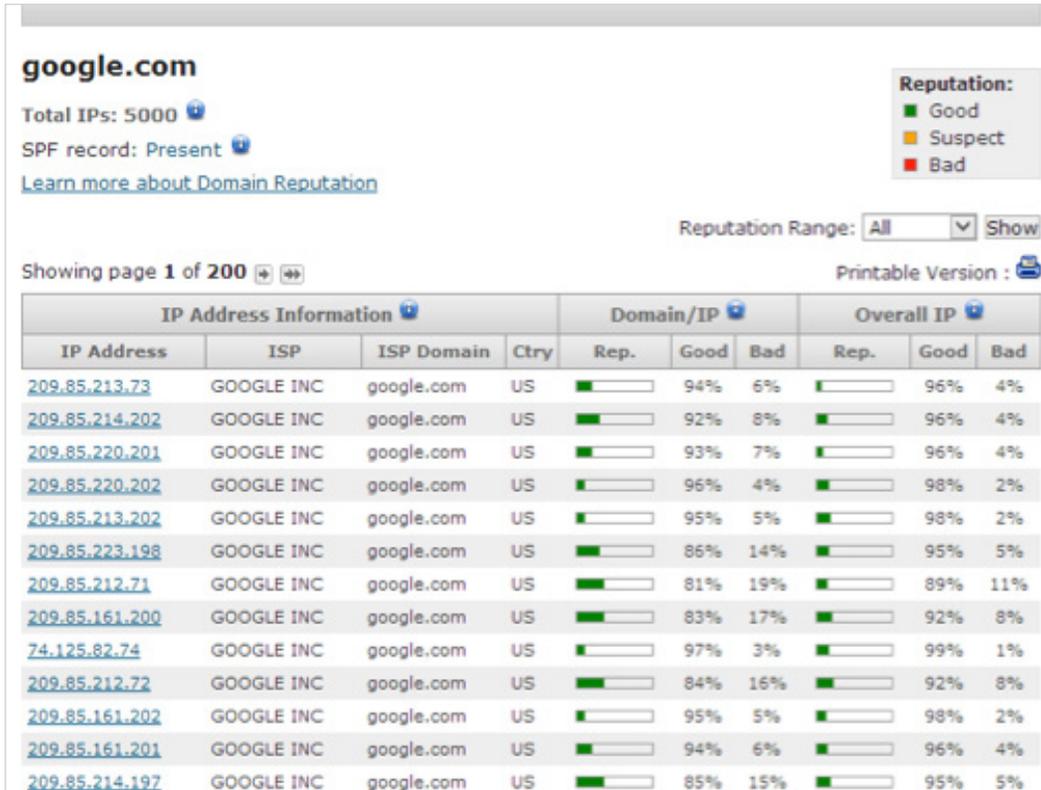
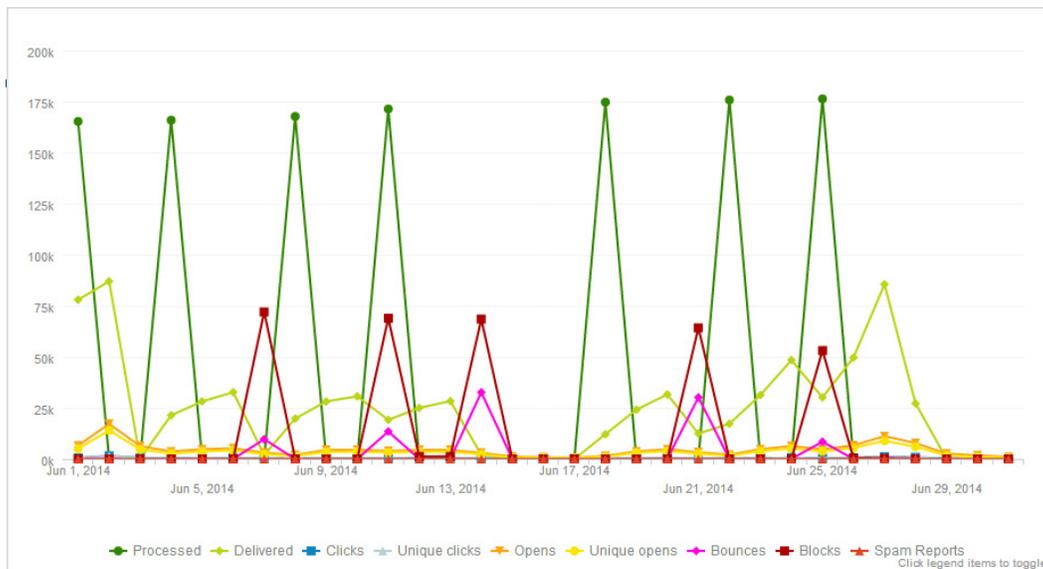


FIGURE 5 IP lookup for ReputationAuthority

## You Can Always Fix Your Reputation

Another way to check your reputation is to find out if you are on any blacklists (a.k.a. blocklist). Blacklists contain lists of IPs or domains that pose a threat to consumer inboxes. Your email service provider may automatically alert you if you're added to one, but it's good to check for yourself. If you are on a blacklist, act quickly. Just a few spam complaints can add a legitimate sender to a blacklist.

There are many blacklists, but you should check to see if your IPs or domains are on any of these popular lists:



**FIGURE 6** Image of SendGrid user who was blocked

### » Barracuda Reputation Block List

BRBL is a free DNS blacklist (DNSBL) of IP addresses known to send spam.

### » Invaluable

The Invaluable anti-spam DNSBL blocks elusive types of spam where the sender is sending unsolicited bulk email and escaping traditional detection methods.



### » MXToolBox

MXToolbox shows you whether or not your domain or IP address is blacklisted and can perform checks on your DNS to see how it is configured.

### » MultiRBL

This free multiple DNS Blacklist service cross-references other blacklists by IPV4, IPV6, or domain.

### » SpamCop

The SpamCop Blocking List (SCBL) lists IP addresses that had mail reported as spam by SpamCop users.

### » Spamhaus

The Spamhaus Project maintains a number of DNSBLs as part of their effort to identify and track spam sources, and provide anti-spam protection. To be removed from this list, visit their [blacklist removal center](#).

### » SURBL

Unlike most lists, SURBLs are not lists of message senders. SURBLs are lists of websites that have appeared in unsolicited messages.



#### Tools to help you earn the reputation you deserve.

It can be time consuming to stay on top of your reputation and monitor your presence on blacklists, which is why it can be good to find a tool that offers blacklist alerts and gives you insight into delivery failures so you can resolve issues. SendGrid has plans that include a dedicated technical account manager who monitors blacklists on behalf of our customers. To learn more about them, [visit our Pricing Page](#).



## 03

## ISP Tools to Help Manage Deliverability

Feedback loops are provided by mailbox providers and ISPs to alert senders if messages are reported as spam. Below is a list of ISP postmaster pages and feedback loops, with links to each (where applicable), to help you register your IP or domain.

Postmaster	Feedback Loop
AOL	
AT&T	
BlueTie/Excite	
Comcast	
Cox	
Earthlink	
Fastmail	
Gmail*	
OpenSRS (Tucows)	
Outlook (Hotmail)	
Rackspace	
RoadRunner (TWC)	
Synacor	
USA.net	
United Online/Juno/Netzero	
Verizon.net	
Yahoo!	
Zoho.com	

**Note:** SendGrid automatically registers its customers for all ISPs that offer feedback loops.

\*Gmail has a feedback loop that is only available for ESPs who are MAAWG members and are approved by Google as good senders.



# Email Deliverability Tactics

## Email Delivery Differentiators by ISP

Worldwide, the number of mailboxes is predicted to reach 4.1 billion by the end of 2015.<sup>7</sup> Yahoo!, Outlook (formerly Hotmail), and Gmail make up the top three ISPs and are likely your primary concern, but other ISPs are also important.

While the makeup of your email list will determine where you focus your efforts, following best practices will get you delivered at practically any ISP. Weighting of delivery criteria varies, filtering algorithms change often, and specific thresholds for each ISP are not publicly available. But remember, best practices are universal. To give you a head start, here are a few tactics from some of the most popular ISPs to help you achieve optimum email deliverability at their mailboxes.

Caution! This doesn't mean that you can forgo one best practice over another. It simply means that one ISP might put greater emphasis on certain practices when delivering mail than another. Following all best practices available to you is the best way to make it to the inbox at any ISP.

---

### AOL

- » Sign up for the AOL Feedback Loop.
- » Authenticate your email with DKIM.
- » Apply for the AOL whitelist.
- » Monitor your IP status <http://postmaster.aol.com/Reputation.php>

### AT&T

- » Separate large quantities of email into sections and deliver at periodic intervals.
- » Don't send email from an IP address where the sender's identity changes often.
- » Include proper header information on all email messages.

### Comcast

- » Sign up for Comcast Feedback Loop.
- » Stay off of blacklists, monitor abuse accounts, and treat attacks seriously.
- » Avoid dynamic IPs.
- » Review error messages sent by Comcast.
- » Watch your sending limits which are determined by SenderScore.



## Gmail

- » Get added to user contact lists.
- » Authenticate your mail with DKIM. Gmail is the biggest proponent of domain reputation.
- » Include a “List-Unsubscribe” header.
- » Watch your engagement levels.
- » Spam communication: Gmail provides a message about why your email was filed as spam.

## Outlook.com (Hotmail)

- » Join the Junk Email Reporting Program.
- » Access the Smart Network Data Services program.
- » Watch your engagement levels.
- » Apply for Yahoo’s Bulk Sender Program.

## Time Warner Cable (Road Runner)

- » Avoid dynamic IPs. Dynamic IP addresses change from time to time making it difficult for you to maintain your IP reputation and for ISPs to know who you are.
- » Handle your bounces, especially ones that tell you that the address does not exist.
- » Separate your marketing and transactional email streams.
- » Maintain a consistent identity when sending by using the same email address and domain.

## Yahoo!

- » Sign up for Yahoo! Mail Feedback Loops.
- » Authenticate your mail with DKIM.
- » Include a “List-Unsubscribe” header.
- » Watch your engagement levels.
- » Send from the same email address.



# Email Deliverability Results

## Getting In Means Staying Out

There are many things you can control when it comes to your email reputation. Paying attention to the signs and maintaining list integrity will go a long way in keeping you out of the spam folder and earning you the results you want.

---

## Pay Attention to the Signs

### »» Focus on negative engagement

Concentrate on building an active audience by monitoring your response rates. If your response rates are good one month, then suddenly drop, analyze the problem and make adjustments. Mailbox providers are looking at engagement data to determine deliverability.

### »» View your statistics by ISP

In addition to segmenting your list by demographics, purchasing behavior, or other criteria, try viewing your statistics by ISP to identify specific problems. For instance, if your Yahoo! open rates drop significantly, determine whether you are bulking, or if your subscribers have lost interest. If Gmail is performing better than Yahoo!, identify the differences and adjust accordingly.

### »» Watch out for email fatigue

Sending too much email to your users can drive high unsubscribe and/or complaint rates. Offer a [preference center](#) so that users can control the flow of their email. Consider your email cadence and focus on relevancy.

### »» Monitor abuse@ emails

Users may be informing you of spam or phished mail coming from your domain so monitor your abuse@ emails diligently. Alternatively, users may reply to your email with complaints or unsubscribe requests providing a first clue that an email campaign is not being well received.

## Maintain High List Integrity

### » Remove role account emails

Remove info@ or admin@ emails from your email file. These role accounts are usually not individual users, so they should not be mailed to. If you can, automatically exclude them from your list, or ask users to provide a personal or business email address. (SendGrid can provide a list of common role accounts. There are about 30 common accounts.)

### » Create a sunset policy

Proactively eliminate users who have not logged into their account or clicked on an email in the last three months. Unused or dormant addresses may be spam traps that can hurt your reputation, so it's best to remove non-responders frequently. Alternatively, send out a reconfirmation or win-back email campaign to see if they want to remain on your list.



**FIGURE 7** Reconfirmation email from Lands' End requesting that the user confirm their email preferences.





### »» **Stop buying lists**

Buying emails from third-party email lists (even Jigsaw) often have bad email addresses and yield high complaint rates. We know that marketers have to grow their email lists and often purchase email addresses, however, we strongly discourage this practice and recommend a more targeted approach. Just one spam trap mistake can impact your domain reputation.

### »» **Don't share your lists**

Sharing email addresses with other parties reduces trust with your company. Even if you disclose sharing in your privacy policy, recipients don't always expect this email, and will mark it as spam.

### »» **Don't hide the "unsubscribe"**

Make it easy for recipients to remove themselves from your list. It's always better for subscribers to opt-out than reporting your email as spam.



## **The Inbox is Your Ultimate Reward**

Here are the five strategic takeaways that should guide your email strategy to make sure you get to the inbox every time:

- » Send the right email at the right time to the right person at the right frequency.
- » Focus on quality over quantity.
- » Send relevant content and monitor your email deliverability.
- » If there is a problem, or you make a mistake, fix it fast.
- » Listen to customers by monitoring engagement.



# Get to Know SendGrid

SendGrid helps you focus on your business without the cost and complexity of owning and maintaining an email infrastructure. We manage all the technical details, from scaling the infrastructure, to ISP outreach and reputation monitoring, to whitelist services and real-time analytics. We offer world-class deliverability expertise to make sure your emails get delivered, and handle ISP monitoring, DKIM, domain keys, SPF, feedback loops, whitelabeling, link customization, and more. To learn more, visit [www.sendgrid.com](http://www.sendgrid.com).



[Learn More](#)



[Read Our Customer Success Stories](#)



[Sign Up](#)

## Sources

1. "Did You Know 144.8 Billion Emails Are Sent Every Day." *Mashable*. BrandSpeak. 27 Nov. 2012. <http://mashable.com/2012/11/27/email-stats-infographic/>
2. "Email Intelligence Report: Placement Benchmarks 2013." *Return Path*. 29 Jan. 2013. <http://landing.returnpath.com/placement-benchmarks-2013>
3. "2012 Websense Threat Report." *Websense*. 2012. <http://www.websense.com/content/websense-2012-threat-report-download.aspx>
4. Bujack, Michal. "SMTP Abuse Prevention in IPv6 Networks Positive Reputation Class of Service Method." *Cloudmark*. June 2012. <http://www.cloudmark.com/en/whitepapers/smtp-abuse-prevention-in-ipv6-networks> [http://www.cloudmark.com/releases/docs/whitepapers/SMTP\\_Abuse\\_Prevention\\_in\\_IPv6\\_Networks\\_v01.pdf](http://www.cloudmark.com/releases/docs/whitepapers/SMTP_Abuse_Prevention_in_IPv6_Networks_v01.pdf)
5. "MAAWG Sender Best Communications Practices Executive Summary and MAAWG Sender Best Communications Practices." *Version 2. Messaging Anti-Abuse Working Group*. Sept. 2011. [http://www.maawg.org/sites/maawg/files/news/MAAWG\\_Senders\\_BCP\\_Ver2a-updated.pdf](http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf)
6. "Email Engagement: Often Talked About, Never Defined." *DMA Email Marketing Council*. February 2013. <http://dmaemailblog.com/wp-content/uploads/2013/02/EngagementDiscussionPaper.pdf>
7. Radacati, Sara and Hoang, Quoc. "Email Statistics Report, 2011-2015." *The Radicati Group, Inc.* May 2011. <http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf>



# 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 eBook will help you manage the critical factors that affect the deliverability of your email messages.**

# Contents

The Importance of Email Deliverability	2
Working with Your Service Provider	3
All About Spam, Spam Traps and Spam Cues	5
The Mechanics of Email Deliverability	6
How Email Sending Schedules Affect Deliverability	9
Email and Content Filters	10
Best Practices for List Management	11
Email Content Tips for Deliverability	13
CAN-SPAM and Other Legal Issues Regarding Email Deliverability	14
The Send Checklist	15
Track Your Response Rates	16
<i>Appendix A: What Spammers Do</i>	<i>17</i>
<i>Appendix B: Best Practices for Retention Email</i>	<i>18</i>
<i>Appendix C: Best Practices for Acquisition Email</i>	<i>19</i>
<i>Appendix D: Best Practices for Transactional Email</i>	<i>21</i>

# 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.

Across all email marketers, bounce rates were significantly better in Q1 2013 (1.9%) compared to Q1 2012 at 3.0%

– 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.

• **Complaints**

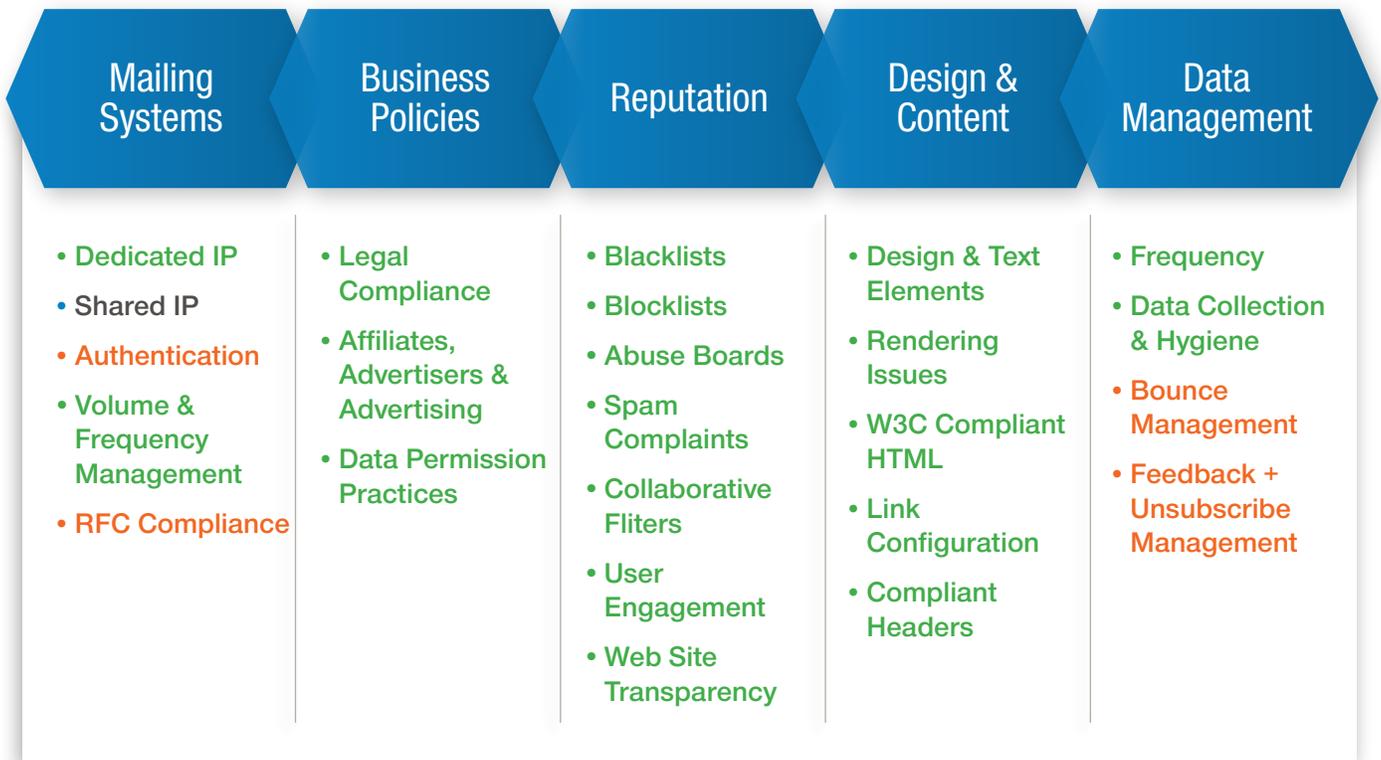
This tallies how many people clicked a spam or junk button link in their email client to report an email as spam or “junk.”

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.



- 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. As a result, many content filters now look at the ratio of HTML comments to visible text. Just having comments doesn’t trigger filters, but having more comments than real text will trigger 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" (2012)

## 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)

## 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](http://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.

## 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.

### 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.

Tips for managing engagement:

**1. Send content 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. 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

## 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."

- 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.

## 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.

## 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
- Other words and phrases that might make your legitimate email look spammy include "free", "bonus", "amazing", "buy direct", "bargain", "no investment", and so on
- 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

# CAN-SPAM

## And Other Legal Issues Regarding Email Deliverability

### Disclaimer:

*Email is governed by laws which vary from country to country. 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 discussion of how legal issues (which can change with little notice) may affect marketers, and is not to be considered or perceived as legal advice. Every organization may be affected differently; 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.

### European Union Laws

Privacy laws in the E.U. are more stringent than in the U.S. Please see Act-On's paper "[The EU Data Protection Requirements](#)" for information specific to the E.U., the U.K., and Germany.

# 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 am, schedule for 9 am 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 clickthrough rates generally range from 5%–15%. Low open and clickthrough 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 clickthrough 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 clickthrough 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 70.5% higher open rates and 101.8% higher click rates compared to Business As Usual (BAU) messages, according to Q4 2012 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.
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 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.

There are many organizations that supply (rent or sell) email addresses that have a level of permission (opted in) that will allow you to send them communications and ultimately utilize this data to grow your house file or generate sales.

### 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 (other than he once attended a webinar or bought a product, which in all probability he doesn't remember), 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. 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.

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

## Appendix C Best Practices for Acquisition Email, Continued

- 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. 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

Adopting and implementing these best practices will give you results and benefits that will affect deliverability, reputation management, engagement, and ultimately ROI.

### About Act-On Software

Act-On Software provides the leading sales and marketing engagement platform for the 21st century business. Simple to operate but powerful in its results, elegant in its user experience and comprehensive in its functionality, Act-On's cloud solution powers over 3,000 companies in their engagement efforts across all stages of the customer lifecycle – attract, capture, nurture, convert, and expand.

The platform's out-of-the-box integrations with popular standalone tools are further complemented by Act-On Anywhere™, a business productivity application that extends the use of marketing automation across web-based environments. Act-On supports an open marketing ecosystem that enables businesses to take full advantage of the latest tools and services available, in the context of an integrated engagement and targeting platform.

+1 (877) 530 1555

[www.act-on.com](http://www.act-on.com)

Copyright © 2015 Act-On Software. All Rights Reserved.





Easy To Use,  
Powerful, Affordable  
Email Marketing!



Get Started  
Today ▶

- [Home](#)
- [Find My IP](#)
- [Hide My IP](#)
- [Change My IP](#)
- [Subnet Calculator](#)
- [Domain Tools](#)
- [Forums](#)

## Email delivery problems explained

+3 Recommend this on Google

With ever growing number of spam emails flooding the Internet, more and more ISPs tighten their email filtering system to prevent spams delivered to their clients. It is virtually impossible to block even 50% of the spams arriving in a mail server, and there will always be false positives (legitimate emails filtered as spams). In an effort to reduce spam emails, the Federal Trade Commission (FTC) passed the [CAN-SPAM](#) Act of 2003, but the Internet spam traffic is still on the rise.

Internet email system is a non-confirming delivery protocol, which means that there is no guarantee that an email sent from you will be delivered to the intended recipient(s). We assume that an email will be delivered to a recipient if no "undeliverable" message is returned to you. However, this is not a safe assumption as large ISPs do filter email messages without returning "undeliverable" message (email blackhole).

Why can't I send email to a particular domain?

Assuming that you can send emails to other users of different domains, there may be a number of reasons why your email is not landing on a particular email address. This is most likely due to misconfigured or missing DNS records, or blocked IP address.

If your email is not delivered to a particular domain, it is more than likely due to a spam filtering. Depending on how email server is configured at the other end, you may or may not receive a bounce email message. If you do not receive a bounce message, it's really frustrating to find that your email is not delivered to an intended recipient. Internet email is unconfirmed delivery protocol, so there is no guarantee that your email will land in mailbox of your intended user. This is especially true with ISPs, and Portals such as Yahoo, MSN, Google and other providers that offer free email services. Those free email providers send and receive millions and billions emails to and from their users, and email spams are one of the most troublesome issues to deal with. To make it tough on spammers, those email providers setup a very strict filtering rules so that any suspicious email will either land in a spam folder or not delivered at all. If so, how do we circumvent such problems as a web host?

1. **Email originated from a spam blocklisted IP address.** If you have a shared hosting plan, there may be a chance that your server IP address may be listed in one or more spam block list such as DNSBL, RBL or

SORBS. Some mail servers treat emails originating from a blocked IP address as spam emails. If you're using email clients such as Outlook or Thunderbird, it is quiet possible that your home PC's IP address may be blacklisted by block lists. The emails sent from Outlook is stamped with your home PC's IP address as the originating IP address, which may cause the email to be blocked by the receiving mail agent. To test if your home IP is the problem, you may try sending the same email from a webmail. Most web hosts provide webmail interface for managing your emails in addition to POP3 and IMAP services. You may look at the mail header, and find an IP address of your mail server (or your home PC) and perform a [spam blocklist check](#) at topwebhosts.org.

2. **Missing Reverse DNS record for MX records.** It is required by [RFC 1912](#) that you have reverse DNS (PTR) records for all of your mail servers. If you do not have reverse DNS entries, your email may not arrive some of the strict mail servers.

3. **Mail server hostname does not match with EHLO/HELO greeting.** The SMTP greeting include 3-digit code, followed by a space or a dash, and the mail server host name. If your email header hostname does not match with EHLO or HELO, your email may be blocked by anti-spam software. This is a technical violation of [RFC 821](#) Section 4.3 and [RFC 2821](#) Section 4.3.1. The hostname given in the SMTP greeting must have an A record pointing back to the mail server.

4. **Missing SPF record.** Many mail servers refuse to accept emails from an IP address without SPF record. Mail servers use [SPF record](#) to help prevent spammers from abusing their system.

Although not directly related, your mail server should be also configured to accept mail to 'postmaster' and 'abuse' email addresses. Mail servers are required by [RFC 822](#) Section 6.3, [RFC 1123](#) Section 5.2.7, and [RFC 2821](#) Section 4.5.1 to accept mail to 'postmaster' account. Similarly, mail servers are required by [RFC 2142](#) to accept mail to 'abuse' account.

## Return Receipt

Some mail systems have a function that can provide a return receipt when the mail is read. The get a return receipt from recipient mail server, you'll have to add special mail header called **return-receipt-to** with return email address where receipt will be sent. Whether you'll get a return receipt depends on the receiving mail system. If receiving mail system does not support receipt, the mail header is simply ignored.

## Undeliverable Mail

If email cannot be delivered, it is usually returned to you with a message indicating the problem. We usually called this bounced email. The sample bounced message below indicates that the mail server requires SMTP-AUTH server authentication. The bounce message is from the **Mailer-Daemon** (mail delivery agent), and it describes the delivery problem with the original email included after the bounce message.

Your message did not reach some or all of the intended recipients.

```
Subject: Subject of the email
Sent: 2/27/2007 8:35 AM
```

The following recipient(s) could not be reached:

```
'test@iplocation.net' on 2/27/2007 8:35 AM
550 5.7.1 ... Relaying denied. Proper authentication required.
```

The bounce message from the SMTP server includes status codes (Enhanced Mail System Status Codes as defined in [RFC 3463](#)) with standard status messages. Each status code is comprised of three digits (i.e., 5.7.1

above). The syntax of the status codes is defined as [class] . [subject] . [detail]. The [subject] status code has three possible values as defined below:

- 2: Success
- 4: Persistent Transient (Temporary) Failure.
- 5: Permanent/Fatal Failure.

The [subject] and [detail] digits provide more detailed status of mail delivery indication. The [subject] sub-code classifies the status, and this value applies to each of the three [class]es.

- 0: Other or Undefined Status
- 1: Addressing Status
- 2: Mailbox Status
- 3: Mail System Status
- 4: Network and Routing Status
- 5: Mail Delivery Protocol Status
- 6: Message Content or Media Status
- 7: Security or Policy Status

The enumerated status codes ([subject].[detail]) describes the detailed status code of the message returned. For further information, please view [RFC 3463](#).

## Common Mail Delivery Problems

Some of the common email delivery problems are listed below.

**User Unknown:** The username portion of the email address (username@host) is no good. The user account may have been expired or deleted.

**Host Unknown:** The hostname portion of the email address (username@host) is no good. The DNS may not be able to resolve host's IP address.

**Mail Could Not Be Delivered:** The message states that the email cannot be delivered for 4 hours (or some duration) means that the DNS knows about the host, but the mail server may be temporarily down. The mail server tries to resend the mail repeatedly for 3-day period, and gives up afterwards.

## Banned or Blocked IP Address

Increasing number of ISPs ban emails from IP addresses that are currently listed in one of the [Spam Blocklist](#) they use. A bounced email message from a blocked IP address may be indicated with the following messages:

451: IP Blocked please visit <http://ORDB.org/lookup/?host=10.0.0.1>

451 Mail from 10.0.0.2/24 refused, see <http://www.spamcop.net/bl.shtml?10.0.0.2>

You may use our [Spam Blocklists query tool](#) to examine whether the IP in question is listed in any one of the Spam Blocklist. If you believe that you're unfairly added to any of the blocklist, you may contact them by visiting respective websites.

### IP ARTICLES

- [What is an IP Address?](#)
- [What is IPv6 Addresses?](#)
- [What is a Subnet Mask?](#)
- [What is a MAC address?](#)

- [What is an Ethernet?](#)
- [What is a TCP/IP?](#)
- [What is a DHCP?](#)
- [What is public and private IP address?](#)
- [What is static and dynamic IP address?](#)
- [What is Ipconfig utility?](#)
- [What is IP Spoofing?](#)
- [My IP address is hacked. What do I do?](#)

Date	Time	Opponent	Action
Tue, Aug 4	7:08PM	vs. KC	<a href="#">Tickets</a>
Wed, Aug 5	7:08PM	vs. KC	<a href="#">Tickets</a>
Thu, Aug 6	1:08PM	vs. KC	<a href="#">Tickets</a>

[VIEW FULL SCHEDULE >>](#) [tigers.com](#)

#### RELATED ARTICLES

- [What is a VPN?](#)
- [What is a Proxy Server?](#)
- [Find IP address of a network printer?](#)
- [Find IP addresses of a private network](#)
- [What is denial of service \(DoS\) attack?](#)
- [How to protect from DDoS attack?](#)
- [How to shape bandwidth?](#)
- [DDoS Protection via Bandwidth Shaping](#)
- [How to wire a RJ-45 cable?](#)
- [Email delivery problems explained](#)

#### SMARTPHONE IP ARTICLES

- [Track lost smartphone w/ IP Address](#)
- [Locate your lost Android smartphone?](#)

## About

Welcome to IP Location, a home of IP Geolocation and IP related resources. This website was built to offer tips, tutorials and articles on IPv4 and IPv6 addresses, and how it relates to TCP/IP and Internet.

## Blogroll

- [Web Hosting Resources](#)
- [Webmaster Resources](#)
- [Free File Hosting](#)
- [Prepaid Wireless Plans](#)
- [Setup Website](#)

## Contact Us

- [Terms of Service](#)



# RPost® Services: Triple Play

## The RPost Difference Service Breadth.

More than 20 innovative services developed over the last 10 years running on RPost's patented Registered Email cloud platform.

## Simplicity. Availability.

Intuitive and effortless user experience; apps for desktop, mobile and web platforms.

## Practical ROI for the Savvy.

Save time, money, reduce business risk, speed transactions; more use brings greater ROI!

## Legal Proof®. Auditable.

Only with RPost do you receive the most robust evidentiary records.

## Authentication. Forensics.

On-demand third-party authentication of message, document content, times, delivery, privacy and legal compliance, e-signature authorship, and audit trail.

## Know & Trust your Provider.

For 10 years we have pioneered messaging innovation trusted by global clients. Count on our team for your project success.

Integrated proof, encryption & e-signatures

**Registered Email® services are secure, authenticated and legal electronic messaging, document, and web services -- the way the world transacts business when it matters!**

**A Problem Solved – The RPost Triple Play:** Who knew what when? Sending standard email is like sending a postcard written in pencil. Message content can be easily snooped or changed with a few mouse clicks without detection. Most of the time it is delivered; but sometimes it is not. Delivery is uncertain and in many cases, untraceable for end users. Using couriers or fax for receipts or to obtain recipient signatures on contracts is expensive and cumbersome. There is a better way; use RPost.



**Legal Proof® records** - RPost proves legal delivery, content and time for any email 100% of the time, regardless of recipient action, with delivery direct to recipient inbox and third party authentication on-demand.



**Compliant Encryption** – only RPost encryption protects the sender from fines associated with data breaches by transmitting encrypted and proving encrypted delivery; proof that any accusations of such data breach must have occurred after the recipient took control – off your watch!



**Authenticated E-Signatures** - obtain recipient electronic signoff on attachments to email. Only RPost authenticates signature, content, timestamp, and signoff audit trail for the highest evidential record of each transaction.

Since 2000, RPost has innovated to offer integrated services that reduce paper, postage, fax, time, risk and cost, while increasing security, and speeding business. Today, the world's largest companies rely on RPost.

## Installs in seconds; and now a free service!

First three users per company can use in any combination:

- 10 Registered Email messages for proof, up to 200MB each,
- 10 encrypted email messages for privacy and compliance, and
- 10 documents e-signed or sent for recipient electronic signature.

(index.php)

[GET MY FREE ACCOUNT \(HTTPS://SECURE.DOCSMIT.COM/ACCOUNT\\_REQUEST\\_FORM.PHP\)](https://secure.docsmiit.com/account_request_form.php)

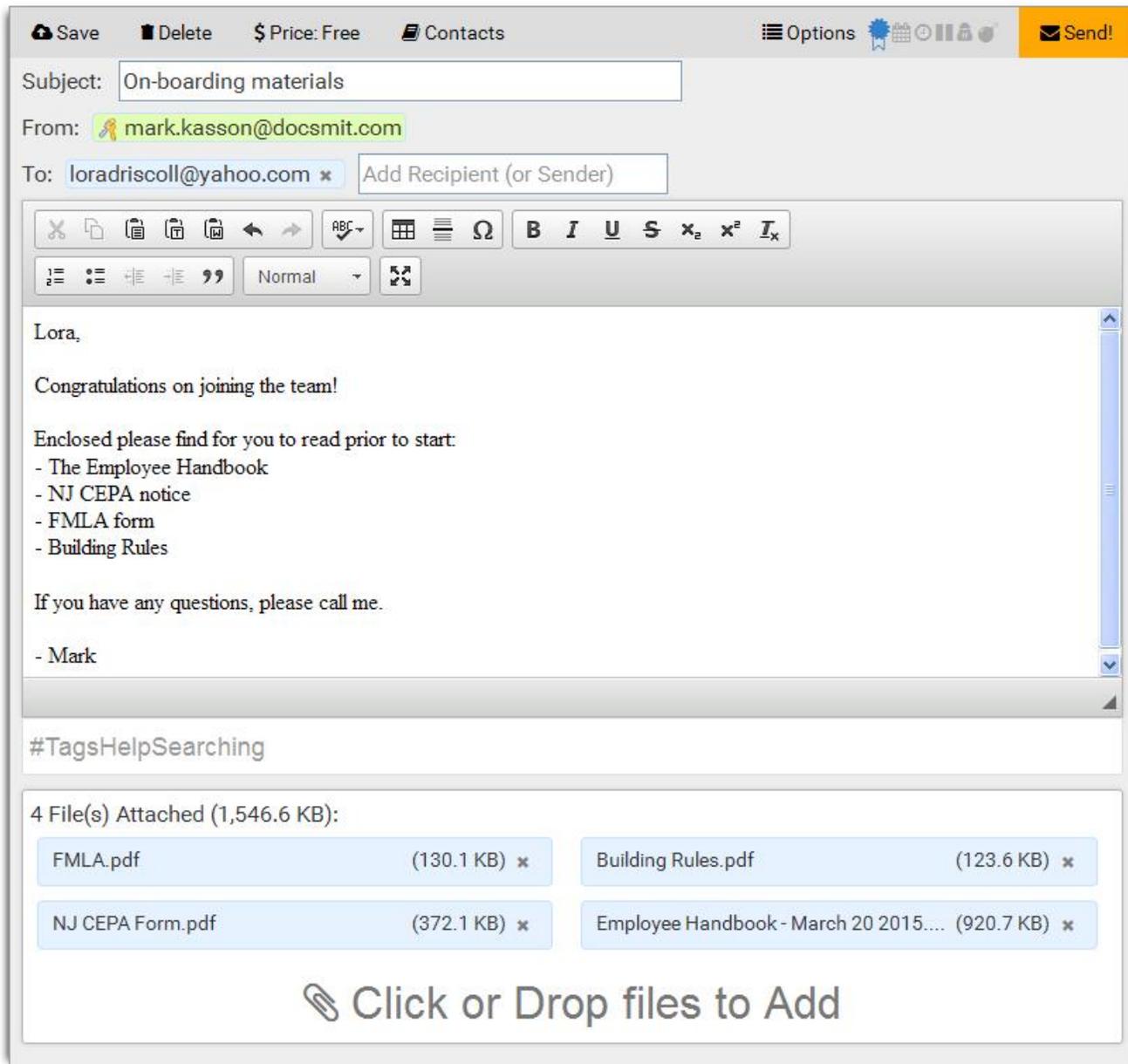
[LOGIN \(HTTPS://SECURE.DOCSMIT.COM/LOGIN.PHP\)](https://secure.docsmiit.com/login.php)

# HOW IT WORKS

Docsmiit acts as a repository in order to document and certify messages. Docsmiit can make authoritative certifications because, like an overnight courier or the US Postal Service, it is unrelated to the message parties and is consistent with the E-SIGN Act and the UETA.



First, you give Docsmmit your message. Drag and drop your attachments - as much as you like!! Specify the recipients and the message is ready to send. Docsmmit will record when it is sent and the contents.





Docsmiit then emails the recipients that they have a message waiting. Only after a recipient "signs for it" - i.e. uses his password and accepts the message - does Docsmiit allow the recipient to access the content.

The recipient gets the message over a secure connection and Docsmiit records the time of this message view (and every message view), then notifies the sender of this first viewing.

## **Prove Delivery and Content**

**Document any message with detailed delivery status and content certification.**



**Grant direct access to data on Docsmmit to eliminate claims of spoliation.**

Mark Flag Reply Add Recip. More Certificate Extend

**Subject :** On boarding information  
**Sent:** 4/13/15, 11:02 AM (Expires: 365 days)

**From:** mark.kasson@docsmi.com  
**To:** forrestblair3@gmail.com  
 Not Signed For  
 Not downloaded yet.

Unclaimed Notice:

Welcome aboard, Forrest!

Enclosed are:

- our Employee Handbook,
- our building's rules, and
- a state and a federal notice.

I look forward to seeing you next Monday!

- Mark

#TagsHelpSearching

**Attached Files:**

File name	size
FMLA.pdf	130.1 KB
Building Rules.pdf	123.6 KB
NLREGA Form.pdf	372.0 KB

Certification gives access to the information about that message, **including the ability to see the exact contents of the message body and attachments**. No overnight courier can ever provide you proof of what was actually IN the envelope!

## TRACKED OR CERTIFIED

### Docsmi has two levels of messages

#### Tracked

---

All messages are Tracked. This means we track when the message was sent and signed for, and the exact contents of the message. Docsmiit retains this information until the message "expires" or is extended.

With a Tracked message, we'll let you know if the message was received, but it won't have our Certification. Some of the information is displayed, but Docsmiit keeps it all in case you need to Certify the message later.

## Certified

---

Certified messages are Tracked messages that have been upgraded. They have longer "lives", but more importantly, you get Docsmiit's certification about the information that was tracked all along.

You can even grant others direct access to the information on Docsmiit.

You can upgrade a message to Certified before it goes out ("Pre-Certified") or even after ("Post-Certified").

## DOCSMIT

[Home \(index.php\)](#)

[How it Works \(howitworks.html\)](#)

[Getting Started](#)

[Pricing \(pricing.html\)](#)

[Blog \(http://blog.docsmiit.com\)](http://blog.docsmiit.com)

---

## SUPPORT

[Support FAQs](#)

[Contact Us \(contactus.html\)](#)

---

## LEGAL

[Terms of service](#)

---

## QUICK CONTACT

Name
Email
Subject
Message

---

**SEND**

---

© 2014 - Present Copyright Docsmit.com, Inc. ALL RIGHTS RESERVED

# Features

**Registered Email®** proof service, the worldwide standard for legal and verifiable proof of email delivery, opening, official time of sending and receiving, associated message and attachment content, with audit trail and authentication.

**Email Encryption**, with a variety of configuration options to maximize security while maintaining user simplicity and flexibility for enterprise organizations. This service is relied upon by some of the world's largest companies, has won the World Mail Award 2011 for security, and was the top pick by The Council of Insurance Agents & Brokers as the insurance industry #1 choice for HIPAA compliant email encryption.

**Legal Electronic Signatures**, with a wide variety of ESIGN compliant authenticated e-signature capabilities for sender, recipient, multi-parties, contracts, PDF forms and messages.

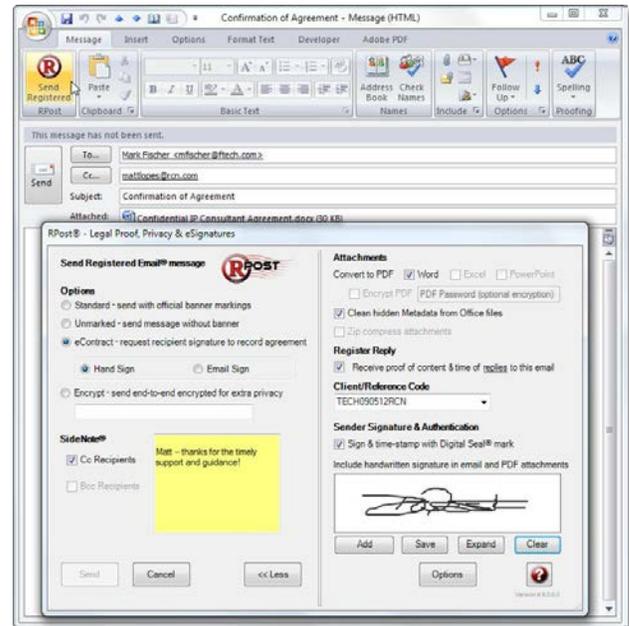
**Digital Seal®** time stamp and message authentication, like a postmark for electronic messages. This service now includes an option to add the sender's hand scripted signature on the bottom of the outbound email and attached PDF documents. The signatures are water-marked with a unique timestamp and the attached document is additionally PKI digitally signed for content integrity authentication.

**Certified Email™** sender authentication services to provide the recipient a simple means of authenticating message author without requiring any recipient software or plug-ins.

**Large File and Document services** transform attachments while en route to the recipient into secure PDF formats with options for meta-data file cleansing, removal of file history, compression and large file transfer up to 200Mb per message.

**SideNote®** service to permit the sender to embed private messages in an outbound email, visible to only the copied recipients as "yellow-sticky note" at the top of the message.

**Records management** reference and matter management, message subject line tagging, special auto-routing of message records, and advanced usage and status tracking reports with a dashboard view of who is using what, when.



## Benefits

- Boosts returns on process improvement investments with new efficiencies
- Reduces legal spend, litigation risk, paper, postage, administrative time and cost
- Proves compliance with data privacy mandates, deadlines for notices, and digital signature laws
- Speeds signoff with intuitive user experience
- Integrates all services into one simple user interface for Outlook, iPhone, Salesforce & more!
- Simple to automate based on message format, content filtering policies or APIs
- Trusted worldwide by the largest mailers, winner 2011 World Mail Security Award



RPost is the global standard for email proof, message encryption and electronic signature services which enable both sender and recipient to prove, sign, encrypt, archive and collaborate across desktop, mobile and online email platforms. Designed for industries such as insurance, financial services, legal, real estate, telecommunications and manufacturing where the speed of contract execution, encryption or court admissible email records is a business requirement. In use with the U.S. Government, global F500 companies and endorsed by influential American Bar associations. RPost, founded in 2000, has been granted 35 patents worldwide and operates in 8 languages.

Los Angeles | Boston | London | Amsterdam | Zurich | Sao Paulo and others...



+1.866.468.3315

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

