WHITE PAPER | AUGUST 2008

Best Practices in Email Marketing

Mastering Your Email Reputation: Seven Strategies for Improving Deliverability

Effective tips and best practices for safeguarding your email sender reputation in today's ever-changing email environment

StrongMail

PUBLISHED BY:

StrongMail Systems, Inc.
1300 Island Drive, Suite 200
Redwood City, CA 94065
Telephone: (650) 421-4200
Facsimile: (650) 421-4201

StrongMail Systems UK, Ltd
Prospect House, Crendon Street
High Wycombe, Bucks
HP13 6LA
Telephone: +44 (0) 1494 435 120

StrongMail Systems UK, Ltd is a company registered in England and Wales at Carmelite, 50 Victoria Embankment, Blackfriars, London EC4Y 0DX. Reg. No. 6398867. VAT # GB 925 07 6228. Trading Address: Prospect House, Crendon Street, High Wycombe, Bucks HP13 6LA.

www.strongmail.com

Table of Contents

Whether you know it or not, ISPs constantly check your reputation as a commercial email sender and filter or block messages accordingly. Gone are the days when receiving domains filtered on content and keywords alone. In fact, according to Return Path[1], more than 80 percent of delivery problems today are caused by the sender's email reputation.

Given the important role that sender reputation plays in getting your email delivered, you need to take an active role in ensuring that your practices don't prevent your messages from reaching the inbox – or being blocked entirely.

Promotional emails aren't the only messages at stake. The delivery of business-critical transactional emails are also affected by your sender reputation. Put simply, you can't afford to overlook this increasingly important component of email deliverability.

While there isn't one standardized formula that all ISPs use to assess your sender reputation, there are a number of metrics and attributes that play a critical role, including complaint rate, bounce rate, sending infrastructure, and spam trap and blocklist inclusions. Understanding the actions and best practices that can have a positive impact is critical, and this whitepaper will outline seven of the most important strategies for measuring, managing and maintaining your reputation as a commercial email sender.

> *"A study by Return Path indicates that more than 80% of delivery problems are caused by reputation."*
>
> *George Bilbrey,*
> *GM of Delivery Assurance, Return Path*

STRATEGY 1: MAINTAIN A CLEAN LIST

List hygiene is one of the most important practices that you can engage in – both from a reputation and results standpoint. Sending to bad addresses not only skews your response rates, it is a core metric that ISPs use to determine your sender reputation.

The following sections offer proven advice for maintaining a clean list.

Bounce Management

Bounce management plays a principle role in list hygiene, as it's the primary mechanism for tracking and responding to the failure codes that you receive from ISPs and other domains. ISPs and other receiving domains issue these bounce codes to let the sender know why a message has failed, and very few follow any standard protocols. As a result, you need to ensure that you have a robust bounce management system that can automatically process and correctly categorize varying bounce codes, so that you can address the causes of those failures.

[1] DM News, "Questions and Answers About Sending Reputation," February 2008

When evaluating your bounce management system and practices, you will want to ensure that they allow you to overcome the following five challenges:

1. Capture All Data Streams. You need to capture all data streams, including asynchronous and synchronous bounces. While most bounce systems capture the immediate synchronous bounces, it's equally important to capture asynchronous bounces, which can be delayed by hours or days.

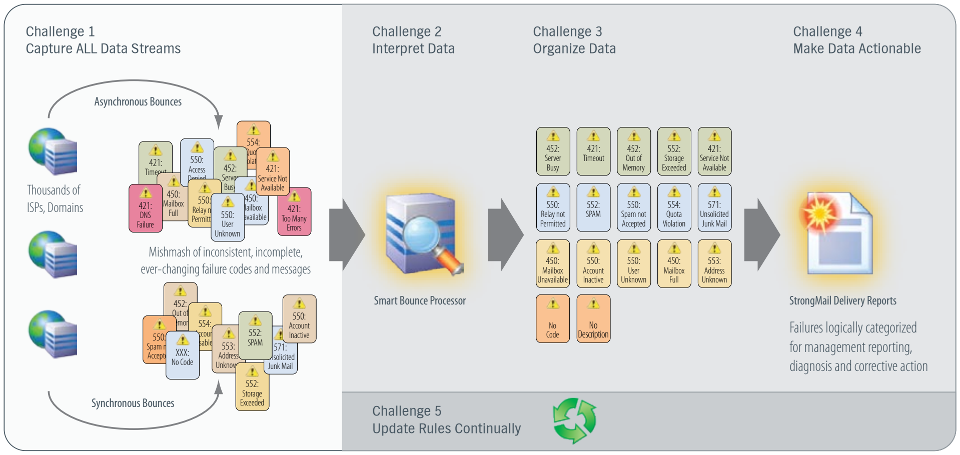
2. Interpret Data. You need to process bounce data and correctly interpret the varying bounce descriptions that come from each receiving domain. If bounces are not properly identified or categorized, problems may go undetected and good records could be invalidated.

3. Organize Data. After acquiring the data, you need to organize it into logical categories, such as hard bounce, soft bounce, block and technical failure. By normalizing the data across ISPs, you can more accurately identify delivery problems.

4. Make Data Actionable. Once organized, you should be able to generate reports that make the data actionable in addressing the causes of failures. The reporting should be user-friendly and available near real-time so you can easily and quickly take action to clean your list, adjust your targeting or modify other practices to improve your deliverability.

5. Update Rules Continually. Unfortunately, the dynamic email environment causes ISPs to periodically update bounce codes, so you need to make sure that your rules are updated regularly to keep up with the changes. Verify that your bounce management system has a process for being continually updated with the latest bounce codes and messages.

> *"Senders should exercise proper bounce management by promptly removing addresses returned as permanent errors by an ISP or other receiver."*
>
> *Email Sender and Provider Coalition, "Principles of Email Sender Reputation," April 2006*



Challenges to Bounce Management

List Hygiene

Bounce management enables you to deal with permanent and temporary address failures, but there are a variety of supplemental list hygiene practices that you should adopt as well. The following activities will help keep your deliverability rates high, and will positively impact your sender reputation.

Scrub Your Lists Regularly. Keep your list as clean as possible by regularly running it against a register of known bad domains and role accounts. The volume and frequency of your mailings will determine how often you want to scrub them. Scrubbing should go beyond removing duplicate addresses.

Remove and/or Correct Bad Domains. Bad domains should be removed or corrected immediately. Closely review your failure reports, identify bad addresses and evaluate whether they are the result of a data capture problem or a non-existent domain. If you're experiencing a high rate of failures, you'll want to determine how those addresses got onto your list and if they're indicative of a data capture problem.

> *"Closely review your failure reports, identify bad addresses and evaluate whether they are the result of a data capture problem or a non-existent domain."*

Remove Distribution Accounts. Mailing to a distribution account is never a good idea. Not only is it the equivalent of sending to "occupant," many ISPs factor such behavior into your reputation. Plus, it's likely to facilitate spam complaints from members of the list. You can easily remove distribution accounts by adding "info@*," "sales@*," and other common addresses to your suppression list.

Remove Inactive Addresses. Review the email activity of your customers and compare open rates with the frequency of the email sent to them. This will allow you to identify inactive customers, which you can then transfer to another list that is designed to reengage them. You will also want to consider removing customers without any opens or clicks within a 12-month period, as sending to these addresses can lead to ISP complaints.

Use Data Checkers. Employing data verification devices at the point of data collection on your website can ensure that email addresses and other information is properly formatted before it is accepted into the database. Identifying the errors at the point of entry gives you the opportunity to have users correct mistakes as they make them.

Feedback Loops

It is very important to set up all available feedback loops with ISPs and other receivers. Feedback loops will enable you to stop sending messages to customers who have indicated that they no longer wish to receive your communications. Not only is it a good idea to respect the wishes of your customers, it is another important practice for maintaining a positive sender reputation. Processing feedback loop complaints demonstrates to ISPs that you are committed to keeping your list as clean as possible and will positively impact your complaint rates moving forward.

While not all receiving domains offer feedback loops, you should identify your top ISPs and determine whether they are available. The following are some examples of popular feedback loops:

AOL: http://postmaster.aol.com/fbl/index.html

Comcast: http://feedback.comcast.net

Windows Live Hotmail: http://postmaster.hotmail.com/Services.aspx#JMRPP

Spam Traps

In order to combat spam, many large ISPs, spam filter providers and related organizations employ spam traps as a way to identify, filter and/or block potential spammers. In essence, spam traps consist of email addresses that conceivably should not be receiving any email. They may be expired addresses or ones created specifically to attract spammers. For the latter, the receiving domain will publish the address in a location hidden from normal visitors but readily accessible by an automated email address harvesting technology used by spammers to cull the Internet.

> *"A typical sender using a legitimate email server will see its deliverability rate drop from 58% to 38% with the inclusion of just one spam trap hit."*
>
> *Return Path*
> *Q2 2008 Reputation Benchmark Report, July 2008*

Sending to one of these spam traps is considered a 'hit' and can severely affect your email reputation and deliverability. In fact, Return Path's Q2 2008 Reputation Benchmark Report[2] found that a typical sender using a legitimate email server will see its deliverability rate drop from 58% to 38% with the inclusion of just one spam trap hit.

Unfortunately, removing spam trap addresses from your list is very difficult, and that's because the originators of spam trap address are unlikely to identify them out of fear of such information getting into the hands of spammers. Thus, you want to take precautions to avoid sending to a spam trap in the first place – and that involves the bounce management and list hygiene practices above, including removing email addresses with the word "spam" in them, as they are often spam traps.

Additionally, you may want to consider a confirmed opt-in process for collecting email addresses to prevent someone from inputting a spam trap address out of spite. If you fear your list is plagued with spam trap addresses, you can re-permission suspect parts of your list, but keep in mind that such an action can lead to the removal of valid addresses from individuals who never take the time to respond.

STRATEGY 2: ADOPT EMAIL AUTHENTICATION

If you aren't already authenticating your email, you need to adopt a strategy today. Not only are ISPs checking for authentication, the act of authenticating your email enables receiving domains, reputation service providers and other related entities to establish your identity and associate a reputation with it. Furthermore, unauthenticated emails are often assigned negative points by spam filters, which can lead to your mail getting sent to the junk folder. The good news is that email authentication is a relatively easy and straightforward process to implement, with the right technology provider.

[2] Return Path, Q2 2008 Reputation Benchmark Report, July 2008

Forms of Email Authentication

There are two forms of email authentication being used today: IP/Path-based and Cryptographic. SPF and Sender ID are the most common IP/Path-based methods. These path-based authentication methods validate the origin of the email by verifying the sender's IP address against the owner of the domain. They look more to where the message comes from while cryptographic solutions focus more on who the sender claims to be.

Cryptographic technologies, such as Domain Keys and DKIM (Domain Keys Identified Mail), rely on a public key that attaches a digital signature to all outgoing email so recipients can verify that the message came from the source indicated.

> *"80% of email from leading brands, banks and ISPs is being spoofed."*
>
> *Authentication and Online Trust Alliance, January 2008*

Email Authentication Adoption

At the 2008 Authentication and Online Trust Alliance (AOTA) Summit, Craig Spiezle, AOTA chairman and director of Windows Security & Privacy Product Management at Microsoft, reported that 55% of all email employs some type of authentication. SPF and Sender ID continue to be pervasive, but DKIM adoption is growing rapidly.

At last year's AOTA summit, it was reported that 85% of Fortune 500 companies were authenticating incoming email. This stat is corroborated by an AOTA January 2008 report that also found that 80% of email from leading brands, banks and ISPs is being spoofed. As of July 2008, Google announced that it is using DomainKeys and DKIM to fight phishing attacks. DKIM's ability to combat phishing has helped it gain additional adoption by such heavyweights as Yahoo!, AOL and PayPal.

For now, because ISPs are enforcing a variety of email authentication technologies, it's best to adopt all the possible options that are available to you. Most commercial-grade email delivery servers allow you to easily implement multiple forms of email authentication by offering them as pre-integrated components within their platforms. If you currently outsource to an email service provider, you should verify that they are able to meet your authentication requirements.

Remember, email authentication is a critical component of safeguarding your company's identity, and ISPs have started to filter email based on varying combinations of the top authentication methods. Furthermore, industry organizations like the Direct Marketing Association highly encourage its members to authenticate their mail to help avoid additional government intervention in the form of regulatory action to curtail spam.

STRATEGY 3: REDUCE COMPLAINT RATES

Your complaint rate is one of the most important metrics used by receiving domains to assess your sender reputation. Developing and implementing a strategy to keep customers from hitting the "this is spam" button will not only positively affect your reputation, it will help you improve response rates and customer satisfaction. While reducing your complaint rates might seem like a daunting endeavor, it really comes down to three things: sending relevant content, managing frequency and respecting your organizations privacy policy.

Relevancy

While marketers typically classify spam as unsolicited email, consumers are not so exacting in their definition. For many consumers, "unwanted" is a more accurate description of spam and the main driver for hitting the "spam" button in their email inbox interface. As a result, marketers need to work on sending relevant messages that are wanted and valued, and that requires tight integration with your customer databases.

> *"Developing and implementing a strategy to keep customers from hitting the "this is spam" button will not only positively affect your reputation, it will help you improve response rates and customer satisfaction."*

While the content needs to be relevant, marketers also need to make sure they're identifying their email in a way that is relevant with a prior interaction. For example, if your company has multiple brands, be sure the "From" line of your email identifies the company with whom the recipient has a relationship. If the consumer doesn't recognize your brand or a prior relationship, they will likely hit the spam button.

Frequency

How often you email your list also plays a role in generating spam complaints. Send email too often, and recipients are likely to hit the spam button to stop the deluge of messages. Testing is key to find the optimal frequency for your line of business. If you're thinking about increasing frequency, start slowly and keep an eye on unsubscribes, complaints, opens and clicks.

Similarly, sending out messages with too little frequency can cause consumers to devalue your messages, or, worse, forget the nature of the relationship they originally initiated with you. Once again, test to find the optimal frequency that results in the highest customer response rate and satisfaction.

Privacy Policy and Permissions

Don't let your enthusiasm for building your list cause you to compromise your data capture processes, and similarly, don't be tempted to skirt your privacy policy to try and generate better results. Either tactic will likely bring about an increase in complaint rates.

When it comes to adding customers to your list, you need to be clear about the kind of messages that subscribers can expect to receive by providing you with their information. Of course, you should never try to be sneaky and 'trick' a customer in signing up to receive promotional messages from you, or even more importantly, from any partner or affiliate organization. This is a surefire way to generate spam complaints. You should also consider allowing customers to change their preferences for the kind of information they want to receive – not only will that help stave off complaints, it will help keep your messages more relevant and effective.

Secondly, you need to respect your privacy policy and make it easy for visitors to view before they agree to give you the permission to reach out to them. If you promote the fact that you don't share your data with third-parties – you need to make sure there are controls in place to prevent that from happening. A June 2008 study by privacy research firm The Ponemon Institute found that while 71% of privacy professionals believe their organizations are respectful of consumers' privacy rights, only 40% of marketers agree.[3]

"Even with the strictest adherence to best practices, there is always a chance that a glitch or malicious act could negatively affect your reputation without you noticing it."

STRATEGY 4: MONITOR YOUR SENDER REPUTATION

Following the best practices outlined in the first three strategies is critical for maintaining a positive sender reputation; however, you also need to take proactive steps to monitor it on a continuous basis. Even with the strictest adherence to best practices, there is always a chance that a glitch or malicious act could negatively affect your reputation without you noticing it.

The following are some resources and recommendations for properly assessing your sender reputation.

Blacklists / Blocklists

You should make a point of checking established blocklists (also known as blacklists) on a regular basis. While ISPs don't rely on blocklists as heavily as they once did, you should make sure your domains and IP addresses aren't listed on the key blocklists that are still used by some ISPs and spam filtering providers.

The following are some of the blocklists that have maintained popularity because of the integrity of their listing and delisting policies.

Spamhaus: *http://www.spamhaus.org*

SPAMCOP: *http://www.spamcop.net*

MAPS: *http://www.mailabuse.org*

[3] The Ponemon Institute, "2008 U.S. Study on Email Marketing Practices and Privacy," June 2008

NANAE

"News.Admin.Net-Abuse.Email" is a newsgroup that focuses on the discussion of spam and poor email practices. This popular online community has a huge membership and regularly tracks the abuse of email systems. You can verify that your company is not a topic of discussion by searching past posts on the NANAE Google Groups, which is accessible via the following website: *http://groups.google.com/group/news.admin.net-abuse.email/topics?hl=en*

SenderScore.org

A service of reputation service provider Return Path, SenderScore.org is a valuable resource for evaluating your sender reputation. By creating a user account, you can enter your domain or IP address and receive a score based on many of the factors previously discussed in this whitepaper. This Sender Score aggregates a large amount of data from ISPs and other organizations to help determine what kind of sender you are. According to Return Path, the higher your Sender Score, the better your email deliverability. Based on a scale of 0 – 100, Sender Score enables you see where you rank against other email senders. Much like a high school grading scale, you can consider a 90 – 100 score an "A." To obtain your score, visit http:*//www.senderscore.org*.

Commonly used by deliverability experts, SNDS lets you see how your sending habits are perceived by the ISPs.

SNDS

Microsoft offers a valuable tool for verifying the status of your sender reputation. Smart Network Data Services (SNDS) is the Windows Live Postmaster Group's method for reviewing your IP address(es). Microsoft introduced the SNDS rating system as a way to fight spam, viruses and other email abuse. As part of SNDS, Microsoft provides mailers with traffic data from all the IP addresses that send mail into their system.

By reviewing this data, you can see how your mail is viewed by an ISP and what is likely happening to it. Finding out is as simple as signing up for the service and verifying your IP addresses. Commonly used by deliverability experts, SNDS lets you see how your sending habits are perceived by the ISPs. You can sign up or find out more information on its official website: http:*//postmaster.live.com/snds/index.aspx*

Key Performance Indicators

As mentioned in the strategy for maintaining a clean list, you need to track your key performance indicators, which include complaints, unsubscribes and inbox delivery rates. By monitoring these on a regular basis and creating trending reports, you will be able to see any changes before they drastically affect your marketing programs.

STRATEGY 5: AVOID ALLIANCES WITH DISREPUTABLE PARTNERS

Before you enter into a relationship with a marketing partner, you should assess their sender reputation in the same manner that you do for your own IPs and sending domains. It doesn't matter how insignificant the partnership might seem, a partner's bad sending reputation can have a lasting negative affect on your programs. For example, if a partner's domain is currently being blocked by an ISP, and you include a link to their site in your own promotional email, your message may be blocked as well.

Similarly, you should also examine the marketing practices of any potential partner. Controversy aside, if you are planning on renting a list or using an email appends vendor, you will want to scrutinize their practices to ensure the quality and legitimacy of their services. Sending to old addresses can affect your reputation by resulting in high bounce rates, while addresses obtained fraudulently or wrongly – even if they are classified as relevant to your business – will lead to spam complaints. However, if you choose to avail yourself of these services, you should always keep these addresses segregated from your house list to avoid compromising its integrity.

The average delivery rates for commercial email servers are 88% versus 23% for illegitimate servers.

Return Path
Q2 2008 Reputation Benchmark Report, July 2008

STRATEGY 6: VERIFY SETUP OF COMMERCIAL EMAIL SERVER

According to the Return Path Q2 2008 Reputation Benchmark Report[4], 46% of all email traffic comes from hosts that should not be sending mail (compromised hosts, dynamic IPs, and other 'non-mail servers'). Furthermore, another 34% of IP addresses were classified as unknown, meaning that either they aren't mail servers or are improperly configured. The study goes on to warn commercial senders that sending from an unidentifiable server is "a recipe for, at best, erratic inbox deliverability." In fact, average delivery rates for illegitimate and unknown mail servers are 23% and 45% respectively.

Legitimate commercial email servers fared exponentially better, with average delivery rates of 88% and low complaint rates of only 1.1%. Consequently, you need to make sure your email is being delivered by a commercial email server that is set up properly to ensure that it will be recognized correctly by receiving domains. If you are sending your email through an outsourced provider, you will want to confirm their settings as well.

When verifying the setup of your commercial email server, you should also consider assigning separate IPs to your promotional and service-based mail streams. Because marketing messages are sent in high volume and are more likely to be miscategorized as spam by recipients, they are more susceptible to reputation issues. By isolating your promotional email streams from your transactional email, you can better protect the reputation of this business-critical communication channel with your customers.

Companies that manage their email in-house with a commercial-grade server for email delivery, integration and campaign management also have the added benefits of real-time reporting, direct integration with customer databases and superior data security by keeping their data behind their firewall.

[4] Return Path, Q2 2008 Reputation Benchmark Report, July 2008

STRATEGY 7: RAMP UP NEW IPS SLOWLY

Whenever you introduce new IP addresses, you need to start sending mail slowly to build a positive reputation with the ISPs. Many of the large ISPs are suspicious of new IP addresses and react harshly to any factors affecting reputation. This is a common anti-spam mechanism that was put in place to combat email abuse. As a result, ISPs are very cautious of allowing large amounts of email into their system from new, unrecognized IPs.

In order to properly build your reputation on new IP addresses, you need to throttle back the amount you send from new IPs until you have established a positive sender reputation. Begin sending to smaller segments of your list and test to make sure those emails are getting delivered – this includes, hard and soft bounces and unknown user and complaint rates. Be sure to start with your most active customers to help reduce complaint rates.

As you continue to see optimal delivery and complaint rates, you can gradually increase the percentage of your list until you get into full production. By doing this in an iterative manner, you allow the receivers to properly assess your reputation and attribute it to your new system.

> *"Unless you pay extra for permanent IPs, you will be sharing your reputation with an ESP's least reputable client, and moving to another provider means building your reputation again from scratch."*

CONCLUSION

Building, improving and protecting your sender reputation involves adopting best practices, using the right technology, and proactively monitoring for and addressing problems appropriately. Once you've established a positive sender reputation, you need to take ownership of this valuable asset to ensure its continued effectiveness over the long-term. StrongMail's commercial-grade solutions for marketing and transactional email give you ultimate control over managing your sender reputation.

Outsourcing to an email service provider can introduce challenges to maintaining your email reputation. Unless you pay extra for permanent IPs, you will be sharing your reputation with an ESP's least reputable client, and moving to another provider means building your reputation again from scratch.

StrongMail's unique on-premise approach provides you with the functionality you'd expect from an email service provider with the control, cost, integration and data security advantages of an in-house solution. Furthermore, StrongMail complements its high-performance servers with a variety of technical and delivery services to ensure proper set up and a strategic ramp up to facilitate maximum deliverability. As email delivery and reputation parameters change, StrongMail continually pushes out Live Updates to keep its delivery protocols current.

For more information about email reputation or how StrongMail can help you meet your email marketing objectives, we encourage you to visit our website (*www.strongmail.com*), or gives us a call at 800-971-0380.

StrongMail

ABOUT STRONGMAIL SYSTEMS

StrongMail Systems provides businesses with commercial-grade, on-premise solutions for marketing and transactional email. StrongMail integrates its proven email delivery, tracking and campaign management software on high-performance servers that are optimized for maximum deliverability.

In addition to providing superior control, security and integration capabilities, StrongMail's in-house approach offers companies a more powerful and cost-effective alternative to homegrown or outsourced solutions. Hundreds of companies worldwide rely on StrongMail's solutions to power their mission-critical customer communications.

A Silicon Valley company, StrongMail is headquartered in Redwood City, CA, and is funded by Sequoia Capital, Evercore Partners, Globespan Capital Partners and DAG Ventures.

www.strongmail.com

Net Atlantic

ABOUT NET ATLANTIC

Established in 1995, Net Atlantic was one of the first email service providers and Web site hosting companies. Net Atlantic's goal is to help businesses and non-profit organizations succeed online with effective email marketing services and Internet tools.

To learn more about Net Atlantic, please visit www.netatlantic.com.

Contact Net Atlantic today.
877-263-8285
sales@netatlantic.com

Net Atlantic, Inc.
10 Federal Street, Suite 26
Salem, MA 01970
P 978-219-1910
F 978-744-0037

www.netatlantic.com