Bulk Email Deliverability Report South Africa 2011

7 December 2010

Bulk Email Deliverability:

Executive Summary

Last year in South Africa 500 million Rand was spent on email and digital direct marketing (Estimate from DMA SA). Internationally email marketing is ranked as the number one interactive marketing format worldwide (Borrell Associates, 2009). Email marketing is also currently ranked number one in terms of return on investment, compared with all other forms of direct marketing (Direct Marketing Association of America, 2008).

Direct email marketing has become an important part of any 360º integrated marketing campaign. Opt-in permission based email marketing is beneficial as subscribers trust the content, therefore strengthening brand loyalty. There is a relationship between the recipient and the email channel which helps cut through the clutter,thus this medium addresses consumers' lack of trust and overall lack of attention to traditional advertising. With the recent rise in the importance of email marketing as part of the marketing mix, bulk email deliverability and sender reputation cannot be ignored.

According to the "Global Email Deliverability Benchmark Report, 2H 2009" study done by Return Path (for the US, Europe and Asia regions) between 14% and 20% of email marketing messages never make it to the inbox. If that international trend holds in South Africa as well, then many millions of Rands are wasted on non-delivered messages each year.

The challenge of getting messages through to your subscriber's inboxes is crucial to achieving the expected ROI. This paper will present the key issues that affect deliverability and suggest steps that can be taken to ensure that one's company has the best email deliverability possible. The subject of bulk email deliverability can be a staggeringly technical one, but at the end of the day deliverability depends mostly on sender reputation and this can be managed through choosing a good technology partner and following good practices.

Email Marketing in South Africa

According to the estimates of the Direct Marketing Association of South Africa, 500 million Rand was spent on email and digital direct marketing last year in South Africa (see table below). This figure excludes agency costs and yet is still an underestimation of total spending; as it only includes costs from members of the Direct Marketing Association (210 companies at the time of survey).

DIRECT MARKETING TOOL	AMOUNT SPENT IN 2009	% OF TOTAL DM SPEND
SMS	R 5 500 000 000.00	36.788%
AGENCY FEES	R 2 500 000 000.00	16.722%
DIRECT TO HOME	R 2 000 000 000.00	13.377%
CATALOGUE	R 1 200 000 000.00	8.026%
MMS	R 1 000 000 000.00	6.689%
CALL CENTRE	R 1 000 000 000.00	6.689%
EMAIL AND DIGITAL	R 500 000 000.00	3.344%
DATA BASE AND ANALYTICS	R 500 000 000.00	3.344%
DIRECT MAIL-SAPO	R 350 000 000.00	2.341%
INTERNET ADVERTISING	R 300 000 000.00	2.007%
MAIL HOUSE AND INSERTS	R 100 000 000.00	0.669%
AMS	R 500 000.00	0.003%
TOTAL DM EXPENDITURE	**R 14 950 500 000.00**	

Table 1: Direct marketing spend in 2009 for South Africa – estimate figures from DMA SA

Direct Mail (through post office) from a volume point of view remains the biggest engagement driver in the direct marketing industry in SA, with email marketing steadily growing behind mobile, telemarketing and direct to home platforms. Email marketing accounts for 3.34% of direct marketing budgets surveyed in South Africa, this relatively low contribution to direct marketing spend is partially due to its low cost. And when marketing budgets are tight, low costs are good.

Internationally, email marketing is ranked as the number one interactive marketing format worldwide (Borrell Associates, 2009). Marketers in the United States claim to enjoy a ROI (return on investment) that is two to three times higher with email than it is with any other form of direct marketing. Email marketing is currently ranked number one in terms of return on investment, compared with all other forms of direct marketing (Direct Marketing Association of America, 2008). Notwithstanding the dynamic differences between markets in SA and the US (or Europe) there remains much potential for growth and further exploitation of this media, especially as the penetration of internet services and broadband increases in SA. At last count the country had 5.3 million internet users, and this is expected to reach the 6 million mark by the end of this year[1].

The low cost and high returns of email marketing are making it a more and more important part of the marketing mix. However, there are still many companies whose email strategy is characterized by high frequency, low value and lack of segmentation. This has partially been fuelled by the relaxed legislative environment surrounding direct and electronic marketing in South Africa. This is changing fast. Never before has one industry been affected by so many new laws, making today's best practices tomorrow's required practices.

Achieving optimal returns from an email marketing program depends to a large extent on deliverability – getting messages through to the recipient's inbox. Deliverability ignores local legislation and is affected by a number of technical factors based on international standards. The single most important factor affecting deliverability is the sender's reputation. This digital sender reputation is based on the mailing practices of the sender and feedback from the mail recipients.

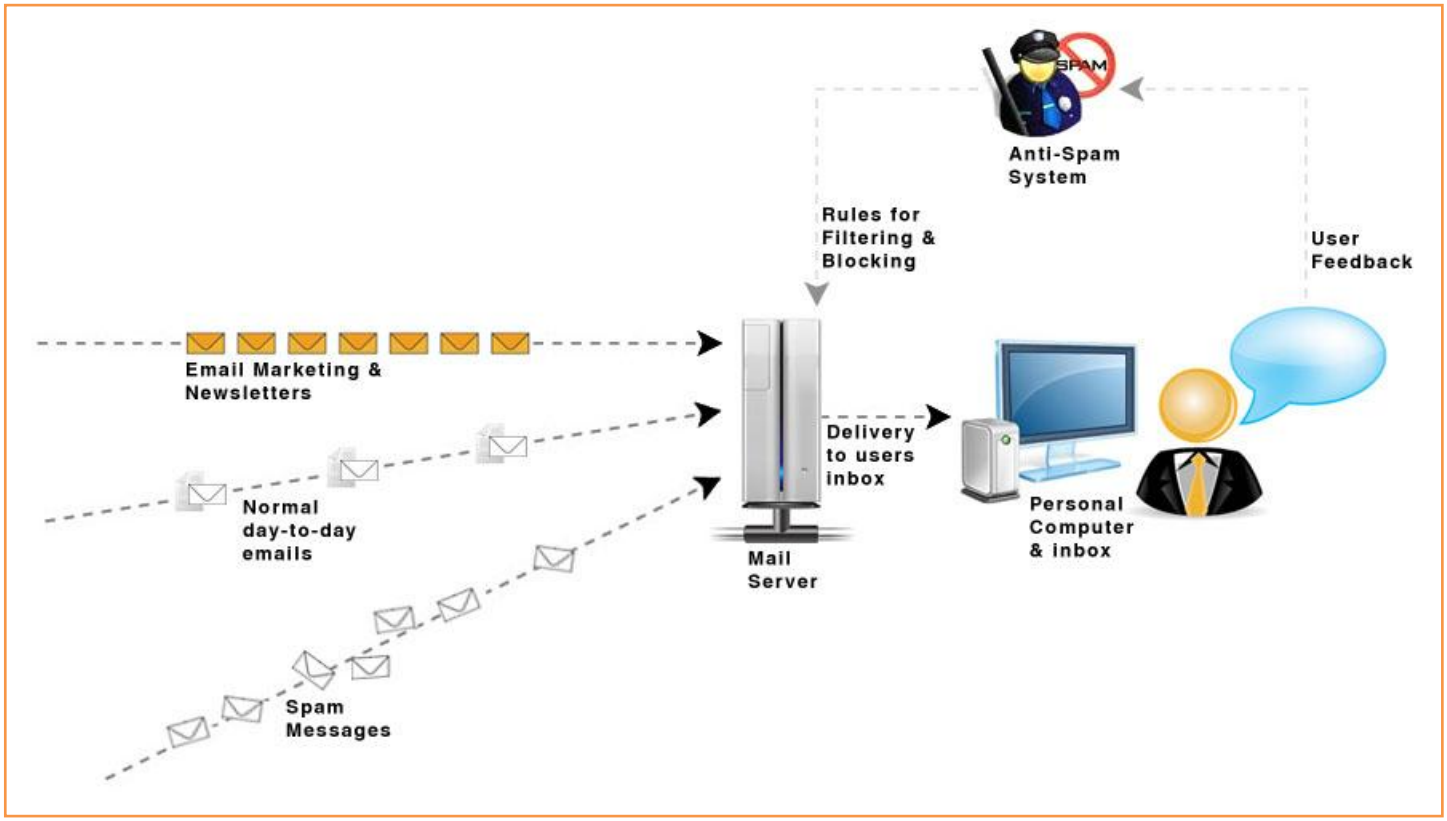
[1] According to the Internet Access in South Africa 2010 study, conducted by World Wide Worx. Accessed on: http://www.southafrica.info/business/trends/newbusiness/internet-140110.htm

It’s all about reputation:

Dealing with Spam

Email has become the standard worldwide for delivering important (even critical) information for business and personal interactions. We rely on email programs and servers to get our messages through, of course for email servers, the job of deciding which emails to allow through and which to block is not so simple.

According to the most recent McAfee Quarterly Threat Report 130 billion spam messages are broadcast every day around the world (and this figure is rising). That’s 68 spam messages per day for each of the world’s 1.9 billion internet users. The reason you don’t see all of those Spam messages in your inbox is thanks to some very advanced spam filtering and blocking technologies active on your ISP (Internet Service Provider) or company mail server.



In order to be able to tell the difference between spam and good email, mail servers and ISP’s will integrate with one of the many Anti-Spam systems that are available. In order to create rules for filtering out Spam messages these Anti-Spam systems rely on user feedback, from the millions of individual email users that are part of their networks. Users provide feedback by reporting messages they believe are spam.

These reports are made in different ways depending on the type of email service the user has. In the case of Gmail, Hotmail, AOL and the like, there is a “Spam” or “Junk” button built into the email interface, by clicking this button when looking at an email a spam report is generated for that message. In the case of users who access their mails on Outlook, Mozilla or a similar email client on their office network or from home; a spam complaint is usually created by forwarding a junk email to the network administrator or ISP’s abuse address.

Alternatively, some reputation scoring companies provide a plug-in, which will integrate with the users email client, adding a button or feature which allows the user to quickly mark a message as spam.

These spam reports that users make are fed back to the Anti-Spam system that their mail server or ISP uses. If too many Spam reports are received the sender of the message will be blacklisted or blocked from delivering future mails.

Where email marketing fits in

Email marketing messages are bulk emails broadcast to recipients on an opt-in or permission basis. Email marketing strategies take two main branches:

- **Two-thirds of all email marketing messages are "retention emails"**; meaning they are sent to a database of your company's previous or existing clients and contacts, with the aim of keeping your brand top of mind and maintaining an interactive relationship with your existing clients. This is important for any company, as acquiring new customers can cost five times more than satisfying and retaining current customers. This type of email marketing is usually referred to as "Email Newsletters" and the recipients are called "subscribers".

- **The other type email marketing messages are "acquisition mailers"**; this type of campaign drives growth in database numbers (gathering new leads and contacts). This usually relies on forwarding and viral sharing; and usually employs other elements of the marketing mix to direct consumers to an opt-in process where their details are collected and permission is obtained to send future communications. An example of this would be an above-the-line marketing campaign that directs consumers to a website where they fill in a form in order to enter a competition; or they are asked to SMS their details to a special number in order to win a prize (or some other collection process). Once the consumers details are captured they would automatically be sent a confirmation email for their entry, possibly asking them to invite some friends to enter the competition. Another example would be competition forms, or club membership forms (filled out at point-of-sales) being captured electronically and emailed an incentivized offer to forward or share a certain promotion.

Once a company implements an email marketing program their database and email newsletter become your own direct communication channel to your customers that can be used regularly to drive sales and strengthen customer loyalty. At this point the issue of email deliverability becomes very important. How does a company ensure that the emails they send out make it to the customer's inbox and do not get lost in the black hole of cyberspace.

In the past most messages filtering was done purely on the content of the message. Today the sender's reputation plays a much larger role than any other factor. When reputation scoring was first employed as a means of blocking spam emails, reputations were simply attached to the sending IP address. More recently, however, sender reputation and blacklisting are being done on the basis of domain addresses (eg: www.mycompany.com) and IP address as well as specific content (eg: phrases, products, HTML patterns and company names).

The technical part:

Factors affecting sender reputation and deliverability

This document is intended to educate marketers and database owners on best practices to improve email deliverability. It is not intended to be technical enough to describe how to build and run high volume email infrastructure, which is the core business of Email Service Providers.

The definition of ‘deliverability’ needs to be cleared up. ‘Delivery’ historically means the number of emails sent less the number of bounces (failed deliveries) that were returned. From a marketing point of view, when speaking about deliverability we are more interested in how many subscribers actually see the message. It is important to note that ISP or mail server message acceptance does not mean the subscriber actually gets the message; there are still filtering processes which determine whether or not the email arrives in the inbox, junk mail folder or just gets deleted by the mail server.

The improvement of deliverability is not just about minimising bounce rates, but also of ensuring that the email ends up in the inbox where it will produce results for the sender. Deliverability is more accurately accessed using an inbox placement rate (IPR). To understand the factors that affect whether or not an email gets delivered to the inbox it is necessary to be aware of who the different Anti-Spam players are, and how they operate. There are several sender reputation providers, spam filter vendors and blacklist operators and each one uses a different approach to tackle the Spam problem.

Different approaches to Spam blocking include:

- Spam Filtering (message content)
- Sender Reputation (complaints from user feedback)
- Blacklist Operators (matching your domain name or IP address)

Overlapping implementation of these approaches is common. Spam filtering and blacklisting serve much the same purpose but use different rules. There is also an overlap on pattern matching too, to illustrate this ‘Spam filtering’ may be matching large red text with the words ‘sale now on’ compared to the ‘Blacklist Operators’ matching a specific domain name or IP address. In essence both of these techniques are fingerprinting techniques. Though for the purpose of this paper, we shall ignore this overlap and look at each approach separately. For example when speaking about fingerprinting of an email, we are referring to the process of matching a company’s name, or a specific pattern of text in the body or envelope of the email. When we talk about Blacklisting, we are referring to the process of identifying domain names and IP addresses through the use of Blacklist Operators.

1. Spam Filtering (messages content)

Historically the primary driver that determined whether ISPs would accept and deliver emails was the content of the email. Certain words or phrases used in the subject line or content of the email would serve as triggers for these content-based filters, and cause emails to be blocked.

There are a variety of spam filter solutions in the market place, some of the best known spam filter providers include: McAfee, BrightMail, Cloudmark, MessageLabs, Postini, Spam Assassin, IronPort and Barracuda (some of these providers also provide reputation and blacklist services).

These spam filters operate at a number of different levels from desktop client filters to server filters. Different Spam filters adopt a range of different approaches for processing emails, for example:

- **Bayesian Filtering** – particular words and sentences have particular probabilities of occurring in spam email and in legitimate email. These filters learn to predict emails to be spam based on user feedback. This feedback is used to identify future spam messages based on the probability of the appearance of different word combinations.

- **Fingerprinting** – this process calculates a checksum that uniquely identifies an email and is used for spotting duplicate messages (or near-duplicate messages – which is how bulk marketing emails are often viewed by the servers that receive and process them). The checksum is computed by evaluating the email's content, and is usually based on: the "Message-ID"; "Date"; "From"; "To" and "Cc" headers together; or on the body of the message.

- **Heuristic Filtering** – works by checking email messages against thousands of predefined rules about the message envelope (header) and content. Each rule assigns a numerical score to the probability of the message being spam. The result of the final equation is known as the Spam Score.

2. Sender Reputation

More recently the primary consideration in whether or not to deliver an email is that of sender reputation. An analogy for this is a financial "credit score" for email senders; this score is decided by a range of factors, for example: the volume of email sent over a certain amount of time; the number of bounce-backs resulting from unknown users; and the number of spam complaint notifications that were received after the broadcast. Sender reputation data is used by ISPs in a variety of different ways when deciding whether to accept or reject email traffic; and may be used in conjunction with other approaches such as spam filtering, authentication, etc.

In the recent "Resender Study" by Return Path (a leading global provider of sender reputation data), it was found that approximately 80% of email delivery problems are directly attributable to a poor sender reputation. It is therefore vital for companies that use email marketing to know what their reputation scores are, and to take corrective steps if their reputation scores are poor.

To monitor the sender reputation score currently being achieved by your email marketing activity, take the IP address that the email activity is being sent from, and run a lookup against that address. Provided that you are generating sufficient levels of email sending activity to register with the monitoring companies, you can check your score online at any of several publicly available websites; two market leaders being:

- Sender Score, operated by Return Path – www.senderscore.org
- Senderbase, operated by Cisco systems – www.senderbase.org

As with Blacklisting (which is discussed later in this paper), sender reputation is not necessarily IP address-specific. Metrics are being managed at domain level, making it important for broadcasters to move away from operating 'good' and 'bad' IP addresses. The factors that the various sender scoring companies take into account vary from operator to operator; and the exact thresholds and formulas are proprietary. Still most of the score operators' websites provide some useful information into some of the key metrics that are used to calculate the reputation scores.

Most common factors affecting sender reputation scores are listed below, the percentages indicated are guidelines and not exact rules[2]:

- **Volume consistency** – your reputation takes a hit if your email traffic has unusual spikes in it. For example if the volume of email sent by an IP address grows by 10% in a month that would be considered reasonable. But if an IP address sends out a million messages every month and then suddenly sends 12 million messages that would be considered risky behavior. Those sending small volumes of email also have challenges establishing a good reputation, as the denominator is just not big enough to be statistically relevant. Low email volumes are sometimes treated with suspicion because spam bots distribute mail across a number of places to stay under the radar. Both these email volume challenges can be addressed by using a reputable Email Service Provider whose combined volume of mail sent from their IP addresses will be consistent and large enough to maintain a good reputation regardless of your individual sending volumes.

- **Attempted delivery to unknown users** – a small percentage of mail bounces (below 10%) is acceptable. But if significant percentage of your mail is bouncing continually because the recipient address does not exist or is incorrect, then that is a problem. It tells score operators that there's something really wrong with the management of your database or data collection system.

- **Complaint rates** – reputation score systems are aware that some spam complaints are just "lazy unsubscribes". So a few spam reports are not going to damage your reputation. It's about keeping the "this is spam" complaints below a certain threshold. Thresholds vary between 2.9% for lower volume senders, to 0.4% for high volume senders[3] who have the potential to do the most harm if they send spam. Generally the trick is to be relatively better than other senders in your volume category. Return Path, for example, records complaint rates across all the commercial emails they track and make the comparative data available to ISP's so they can decide for themselves what level is acceptable and at what level to block mails.

- **Spam trap hits** – these are email addresses that should not normally end up on an opt-in list. They are either created specifically to see if anybody emails them or are dormant email accounts converted to spam trap email addresses for the same purpose[4]. The threshold for spam trap hits is very low, in some cases hitting a single spam trap is enough to downgrade your reputation (or put you on a blacklist). If your company is acquiring its databases through a genuine double opt-in process and keeping lists up to date you shouldn't ever hit any spam traps. Your ability to avoid or eliminate spam trap addresses is a great indicator of your data collection process.

---

[2] Based on the Return Path Certification documents: *RPC_Certified Level Standards and FAQs*; and *Best Practice Guide*; as well as "Email Sender Reputation: expert interview" with Ken Takahashi from Return Path (http://www.email-marketing-reports.com/deliverability/reputation/sender-reputation.htm).

[3] Return Path Certification document: RPC_Certified Level Standards and FAQs.

[4] DMA UK Deliverability White Paper Review, page 10; and Email Deliverability Guide for the Asia Pacific Region 2009, page 6.

- **Permanence** – The longer you've been sending email reliably and safely from a particular source, on a fixed and unchanging IP address, the better your likely reputation. It is about establishing a track record of good sending behavior and accountability for your actions.

- **Infrastructure** – not all bulk email system are created equal. Reputation is affected by the technical ability of your sending infrastructure to do all the things that are expected of a high-volume sender[5]. For example: reverse DNS listing; authentication (Sender-ID/SPF[6] and DKIM[7]); proper bounce handling (like removing addresses that repeatedly bounce), security of the sending mail server (e.g.: open relay servers are open to exploitation from spammers, and therefore considered risky); providing a suitable and easy unsubscribe method (this can sometimes be subjected to a manual human review); and others factors that are core to the Email Service Provider business.

Maintaining a good sender reputation is a joint responsibility of the marketer and their technology partner (Email Service Provider). While an Email Service Provider (ESP) will be responsible for aspects such as infrastructure, bounce handling and ISP relationship management, the marketer will control how the data is being collected, frequency of contact, and quality of targeting. All of these factors affect sender reputation, and both parties have vital roles to fulfill in this regard. By taking note of the factors that affect sender reputation, you can identify where your email program is falling short, and take appropriate action to rectify those shortcomings.

3. Blacklist Operators

A “Blacklist” is a generic name for a list of domains, IP addresses or URLs that originate with known spammers. These lists are either hosted internally on mail servers or available on the internet and are most commonly used to block email from senders listed on them.

Blacklists contain records of e-marketing activity that has been identified as spam-like in nature. ISPs, spam filter vendors and domain administrators will use this information as a guideline to determine whether they will deliver or reject incoming emails. Blacklisting is usually done automatically in real time as complaints are received, which means that a sender can be blacklisted while his campaign is still busy going out, so the later part of the campaign experiences poor deliverability because of complaints received during the earlier part of that campaign.

In some cases the email sender can be reported directly to the blacklist operator. Alternatively, the blacklist can be managed independently via consumer feedback, with the lists being populated on the basis of the operator’s own observations, spam traps and expertise.

There are different types of blacklists that exist[8]:

[5] DMA UK Deliverability White Paper Review, page 9; and Email Deliverability Guide for the Asia Pacific Region 2009, page 3.
[6] SPF = Sender Policy Framework
[7] DKIM = Domain Keys Identified Mail
[8] Deliverability Guide for the Asia Pacific Region 2009; and Wikipedia, Comparison_of_DNS_blacklists

- **Domain Based Blacklists (RHSBL):**
  Domain based blacklists capture domain names that are associated with known spammers. These lists are sometimes referred to as RHSBLs (Right Hand Side Blacklist) as they list the 'right hand side' of the 'from' or 'reply to' email address – the domain name after the '@' sign. Domain based lists are not always effective as most spammers either use forged 'from' addresses or use 'from' addresses containing popular freemail domain names, such as @gmail.com, @yahoo.com or @hotmail.com. Many anti-spam experts believe that domain tracking itself is only effective to a certain extent, as professional spammers are known to constantly change domains.

- **IP Based Blacklists (DNSBL):**
  IP based blacklists identify IP addresses or IP ranges that are associated with known spammers or unused IP spaces. The technology that enables them is built on the Internet Domain Name System (DNS), hence these lists commonly referred to as DNSBLs (Domain Name System Blacklist). Most modern mail servers have DNSBL support that allow a mail server administrators to block mail from IP addresses listed on a specific DNSBL in order to reduce levels of spam received. In addition, DNSBLs are often used as a part of spam scoring systems (spam filtering). If you're listed on a DNSBL that is referenced in a spam scoring system, your spam score could be increased (the amount of the increase varies). If this increase, in addition to other scoring tests performed, makes an email's score rise above a certain level it could be discarded or routed to the spam folder. There are many DNSBLs, all with different policies for adding IP addresses to their lists. Some blacklists apply very radical list policies and are poorly maintained, these blacklists can contain addresses that are associated with legitimate mail and as well as spam. As such, these poor quality blacklists see limited usage from ISPs who want to ensure that legitimate mail is delivered. Other DNSBLs are more conservative, endeavoring to only list actual sources of spam. These more conservative blacklists are more broadly used by ISPs and mail servers.

- **URI Based Blacklists (URI DNSBL):**
  URI (Uniform Resource Identifier) DNSBLs list domains and IPs that are found within the body of spam emails (but generally not legitimate emails), instead of listing sending domains or IPs. This type of blacklist is considered very effective and is used by many ISPs and servers. URI DNSBLs were created when it was determined that spam filters were failing to trap significant volumes of spam during the short time frame between the first use of a spam-sending IP address and that IP address being listed on major sending-IP-based DNSBLs. In many cases, domain names or IP addresses (collectively referred to as a URIs) in the body of these messages can be identified as originating from previously caught spam and not legitimate email. Therefore, when a spam filter extracts all URIs from a message and checks them against a URI DNSBL, the spam can be blocked even if the sending IP for that spam has not yet been listed on any sending IP DNSBL.

Some of the better known blacklist operators are: Spamhaus (www.spamhaus.org) and Spamcop (www.spamcop.net). A comparison of different blacklists and their operator policies is available on Wikipedia: http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists.

The most common causes of Blacklisting are [9]:

- **User Complaints** – As with sender reputation user complaints and spam reports lead to blacklisting. Most often blacklisting occurs against emails with complaint rates of over 1%.

- **Spam Traps** – Spam traps are widely used by blacklists, some operators search for hits on multiple traps, some use spam traps in accordance with other metrics, but, generally speaking, hitting a spam trap (sending an email to it) leads, directly or indirectly, to being blacklisted.

- **Infrastructure and security** – Most blacklists disallow email sent from servers that are not secure (eg: open relay servers, open http proxy servers). Many blacklist operators also treat servers with non-conforming reverse DNS service; poor RFC standard compliance; or dial-up and DHCP IP addresses that are not meant to be initiating SMTP connections (and other technical shortcomings indicative of compromised systems) in the same way. Once a mail server is detected or reported with these types of shortcomings, they will be added to one or more blacklists, and other e-mail servers using those lists will reject any mail coming from those sites.

In South Africa the following anti-spam systems have a large presence (but are by no means the only ones) so their policies have a significant effect on the deliverability of mails to South African inboxes: Barracuda, SenderScore (Return Path); SpamHaus; SpamCop ; TrendMicro; SORBS and uribl.com. Their policies conform to the factors for filtering, reputation scoring and blacklisting discussed above. Understanding how different Anti-Spam systems and blacklist operators rate senders and decide which mails to block, e-marketers then need to understand what steps should be taken to make sure that their broadcasts are compliant with the requirements of these key players.

[9] Deliverability Guide for the Asia Pacific Region 2009; and Wikipedia, Comparison_of_DNS_blacklists

Ensuring good email deliverability:

Follow good practices

According to “The Global Email Deliverability Benchmark Report, 2H 2009” study done by Return Path, the effective delivery to inbox rate (“Accepted Rate”) stands at around 80.1% for Canada and the US; 85% for Europe; 86.9% for Asia Pacific (no figures for Africa and Middle East unfortunately). They found that between 2.5-3.6% of mails landed up in the junk folder and the remainder was dropped or “missing”. The “delivered” metric that most bulk mail systems report tends to be about 95% to 98%, but this metric is actually an indication of the bounce rate rather than inbox delivery rate.

Why is inbox deliverability so low? Many senders are still resistant to implementing the best practices that make email deliverability more likely and more consistent. There are many companies whose email strategy is characterized by high frequency, low value and lack of segmentation. Even most of the top brands are missing basic best practices like welcome messages, efficient opt-out procedures, appropriate permission levels and value propositions for their mail programs.

By choosing the right technology partner (Email Service Provider) and following good practices as recommended below most e-marketers should be able to produce delivery metrics that are comparable to, or better than the above “accepted rate”.

Questions to ask your Email Service Provider

We are approaching an email marketing world where the only way to be truly successful is accepting accountability, using a consistent identity, accepting your reputation and doing your best to keep that reputation positive. For any commercial sender of high volume email, ensuring that proper authentication standards and technology implementations are in place is the core business of your Email Service Provider (ESP).

The policies and practices of your ESP (or own delivery infrastructure) will have an impact on your deliverability. Here are some questions you should ask when choosing a technology partner for bulk email delivery:

- **How is Authentication implemented?** Are Sender-ID or Sender Policy Framework (SPF) records in place to validate the emails delivery path? Are Domain Keys Identified Mail (DKIM) being utilized to allow authentication of each email message using signature key which is generated by the sender and included within the email header? If authentication is not implemented according to standards mails may be rejected.

- **How are bounce backs handled?** Bounce back messages or non delivery reports coming back from mail servers should be accepted by the sending servers, and should be reported on. Email addresses in your database that perpetually bounce should be removed automatically to ensure that lists stay clean and do not harm your reputation.

- **How are unsubscribes handled?** Mandatory unsubscribe links should be enforced on all campaigns. The unsubscribe link should be transparent and easy to use. The unsubscribe feature should be advanced enough to reliably handle an unsubscribe for a recipients who exists across multiple lists in your database. The unsubscribe header tags which web email programs (like Hotmail and Gmail) require should be implemented on all mails.

- **What is the ESPs anti-spam policy and how is this enforced?** If the ESP does not have a strict anti-spam policy it is likely that some of their other clients follow dubious mailing practices, sharing IP addresses and tracking domains with bad senders will negatively affect your deliverability. Your ESP may be able to offer you your own set of sending IP addresses and domains. Senders who prefer not to share IP addresses (and therefore reputation) with other senders, should take care to ensure that their own reputation is sufficient to ensure good delivery.

- **How does the ESP monitor and resolve Blacklisting and Sender Reputation issues on their server IP addresses and tracking domains?** ESPs should have an established reputation and relationship with the most important Blacklist Operators and Reputation data providers. Blacklistings or poor reputation issues should be picked up and resolved quickly.

- **Are Complaint Feedback Loops (CFLs) monitored?** CFLs provides the sender with the email addresses of the complainers so that they can exclude (unsubscribe) them from further mailings, this helps eliminate spam-complaints that are actually just lazy unsubscribes. Currently AOL, Yahoo, Hotmail and a few others operate a complaint feedback loop program, but many ISP do not provide this feedback so it is impossible to eliminate all complainants in this way.

What about the little guys? Smaller businesses often cannot afford deliverability audits and certification; and their volumes may not be high enough to register a unique sender score, so they remain an unknown sender whose deliverability is biased by risk. Many ESPs gear their offerings to small businesses as well. The ESP takes on the role of that deliverability consultant and the ESP's combined volumes work in your favor, provided your ESP follows best practices and monitors usage of their service.

If you happen to be sending mail out from your own server it is important to ensure that the setup and configuration of your infrastructure conforms to standards and best practices. You can get hold of documentation on how best to configure your infrastructure from some of the major ISPs.

Recommendations for improving deliverability

In order to maintain a good reputation, avoid blacklisting and ensure better email deliverability there are a number of best practice recommendations that should be implemented.

1. Improve data collection and check opt-in history

Maintaining a high quality of the email address data being collected for your email marketing program is the most important thing you can do to improve deliverability. Good opt-in and opt-out policies and practices, together with regular data maintenance, are the most effective ways to maintain high data quality.

If your company is using an external data acquisition source it is important to work closely with the provider to determine their opt-in policies and the quality of their lists. A list hygiene policy should be enforced that requires: proof of opt-in; date when the email addresses were acquired (the age of the list); the last time the list was emailed. This is particularly important as records that have not been emailed for a significant period could have: been converted into spam traps or lost interest and forgotten about that subscription and start reporting mails as spam. It is important when acquiring a database that the person opting in, is opting in to the brand from which they will receive communications in future. If recipients do not remember agreeing to receive communication from your brand they will perceive your emails as Spam, even though they have opted in. It's a perception issue.

If you are collecting opt-in email subscribers through your own marketing and lead generation efforts the following should be implemented at the point of data collection:

- Strengthen the permission mechanism: There is a proven relationship between the permission mechanism that is used to sign up the new subscriber and their responsiveness. Positive opt-in (where the box is unchecked) is preferable to passive opt-in (where the box is pre-checked). Double opt-in (where a confirmation email with a link to activate the registration is sent after signup) is preferable to single opt-in. This is a best practice recommendation and not a legal requirement in South Africa. Go for the strongest mechanism that your program will support.
- Double entry of the email address: Many incorrect email addresses (resulting in unknown user bounce backs) are simply typing errors. This can be overcome by requesting the double entry of the address, with the two fields being cross-referenced against each other; it is highly unlikely that the same mistake will be made twice. Some ISPs track common mis-spellings ("hotmial" instead of "hotmail") as a means of tracking whether or not appropriate list hygiene is being maintained.
- Send a validation email: Even if double opt-in is not being used as the permission mechanism, it is good practice to generate a confirmation or welcome email. This has some useful side benefits:
  - Immediate validation of the new email address
  - Opportunity to positively reinforce the initial brand experience
  - Request to be added to the trusted senders list
  - Apply progressive registration approach to obtain further details about subscriber

Good list hygiene prevents your list from becoming cluttered with invalid email addresses that increase the number of hard bounces from your campaigns and contribute to poor reputation or blacklisting. Perform data audits before sending to lists to eliminate poor addresses data such as:

- Duplicate addresses
- Known previous bounce back records
- Invalid structure (no "@" sign etc.)
- Junk entries (dfgdfgdfg@dfg.hj)
- Common mis-spellings
- Profanities
- Potential harvested addresses that have found their way onto you list ("sales@", "info@", etc.)
- Foreign country addresses (potentially no relevance to local campaigns)

If your list contains bad data like this you should question the integrity of your database (and list broker) and scrutinise your optin procedures very carefully.

2. Manage expectations and relevance to reduce complaint rates

Subscriber expectations should be managed by explaining clearly and concisely on a registration page (or data collection point) exactly what they are signing up for; how often they can expect to hear from you; and what type of communications you will be sending them. These commitments to content and frequency should then be followed closely to ensure subscribers receive what they perceive to be the relevant messages they signed up for.

Registration pages should also offer the subscriber control over the messages they receive. Individual preferences settings such as message format (html or plain text), communication frequency and product or topics of interest, allow the customer to personalise the emails they receive to their taste, making them more relevant and reducing the likelihood of future complaints.

Remind your subscribers why they are receiving your messages and re-confirm their email address and mailing preference regularly. Ask for feedback – by learning about your audience and using that information to improve your future message content and targeting your communications, you can both limit complaints and improve response rates.

Be consistent with the “from name” and “from address” for all email communications, this generates increased recognition as users become familiar with them and they can be added to the recipient’s trusted senders list.

3. Unsubscribes and complaint handling

All email marketing messages must include a means for the recipient to opt out. This unsubscribe mechanism should not be hidden in the email message and must, at minimum, be website and/or email enabled (ie: clicking an unsubscribe link or replying with “unsubscribe” in the subject line). The unsubscribe process should be clear, easy to follow and tested regularly to ensure it works. If someone tries to unsubscribe by following your procedure and it fails; or worse, they unsubscribe and still receive communications from you, they are likely to report your messages as spam, regardless of the opt-in procedure they went through..

It is human nature to take the path of least resistance. To some subscribers the spam button is just the “lazy man's unsubscribe button”. If you are receiving a lot of complaints you may consider putting the unsubscribe link at the top of your mailers (as well as in the footer) so that lazy recipients don’t have to scroll to the bottom of the mail to unsubscribe.

Implement a fair, effective, confidential and easy to use complaint-handling system (like sending an email to “complaints@mycompany.co.za”). Any complaints from individuals regarding your communications to their email address should be dealt with courteously and within a reasonable time frame.

Simply put, make it easy for people to leave your list, when they want too.

4. Check inactive recipients for Spam Traps

Inactive subscribers (those who don't open emails or click on any links over an extended period of time) can be linked to dormant accounts and these accounts are increasingly being used by ISPs to create spam traps.

This is a particular threat with regards to acquired or revalidated addresses; such an email address that doesn't open or respond to emails over several consecutive campaigns should be monitored closely and perhaps taken off the list to limit the risk of hitting spam traps. While it may not be possible to identify the actual addresses that are causing problems, segmentations can be introduced to quarantine the address and narrow down the options.

Inactive email addresses that have opted in to receive your marketing messages present a lower risk of having been converted in to spam traps in the short term, but should generally be removed from a list after 12 months of inactivity.

5. Monitor Your Sender Reputation and blacklists

Sender reputation is the single most important factor used to determine email acceptance by ISPs. A sender's reputation is monitored by a variety of factors and is linked either to the domain or the IP address from which the emails are sent or a combination of both. ISPs often use external companies to provide sender reputation data so that they can screen emails against it.

Many of these suppliers of sender reputation offer lookup facilities where users can enter an IP address and get a free report of their current sender reputation status. Sender Score (www.senderscore.org) and Senderbase (www.senderbase.org) are two of the better-known sites. Typically, these sites will provide a high-level classification of how the email traffic originating from that IP address is currently ranked. In the case of Sender Score, this is on a scale of 0-100 (with 100 being a best case scenario), while in the case of Senderbase it's a traffic light-style system – good, neutral or poor. Subscribing to both of these services will allow you to get more detailed information on your reputation.

Blacklisting needs to be checked on the various blacklist operator's websites. There are many blacklists in existence, although some are more influential than others and the impact of being listed depends on the list that the sender finds himself on. There are between five and ten very important blacklists which are referenced around the world by many different organisations and spam filters. Links to these companies can be found in the proceeding section under "Blacklist Operators".

Any sender experiencing delivery problems would be well advised to check if they are being listed on any of the major blacklists or have a bad sender reputation score. Before removing a bad senders blacklisting or reputation entry the operator will often seek reassurance that the infringement (cited as the reason for creating the listing) doesn't happen again. That might require the sender to provide evidence of good practice or simply be based on the acceptance of trust and assurance that no further infringements happen. Repeat offenders will find the operators very reluctant to remove the listing.

6. Get the right infrastructure in place

Responsibility for infrastructure setup and following standard protocol will depend on whether the sender is using an ESP, or relying on its own email broadcasting infrastructure. Outsourcing the mass email delivery to an ESP makes sense for many companies but care should be taken in choosing the right partner. If your company will be relying on its own systems it is important for the responsible technicians to remain abreast of new developments in the field and keep the system up to date with standards.

Whether you use an ESP or own infrastructure you may want to consider registering a sub-domain specifically for email campaign activity. The benefits obtained from doing this are:

- The sub-domain can be linked to the broadcast server for SPF / Sender-ID needs
- Generates increased recognition as recipients become familiar with the sub-domain
- Can be added to the recipient's trusted senders list
- Allows domain-specific sender reputation monitoring

7. Conduct Pre-Broadcast Testing

In all aspects of email marketing it is a good idea to test before sending out a campaign. This is also true when trying to avoid delivery issues. Testing your message against content filters will help spot any content related issues before the broadcast. Other factors, not necessarily related to delivery, can also be checked at the same time. For example, different webmail programs can display emails in different ways, testing this will ensure your message renders correctly.

Even if pre-broadcast testing is conducted many delivery issues can occur after a campaign has been sent or part way through the broadcast. For this reason it is a good idea to monitor the percentage of messages which are being delivered into the inbox versus the junk folder with the major ISPs.

There are a number of tools available through ESPs and delivery specialists such as Return Path and Pivotal Veracity, which check this for you. They work by seeding campaigns with a large number of sample addresses for each ISP and then automatically login and check whether they were delivered or not. Using these results the tools can provide an estimation of the 'Inbox placement rate' or 'ISP acceptance rate' (not to be confused with delivered rate). By monitoring your inbox delivery rate you can quickly spot when blockages might have occurred.

8. Certification

There are a number of certification schemes in operation which allow a sender to bypass spam filters. They all operate through a process of the sender paying a fee and a verification process in order to certify that they are a good sender and follow best practice methods for sending bulk email communications. Once the certification is in place the senders can benefit by bypassing the spam filters. There are two main certification programmes currently available. Return Path Certification is offered by Return Path and Certified Email by Goodmail Systems. Annual license fees must be paid (based on volume of emails sent) to maintain certification. Most of the ISP's (and mailboxes) that apply certification whitelisting are currently located in the US, Europe and Asia Pacific[10].

[10] Return Path Certification Inbox Coverage: http://www.returnpath.net/commercialsender/certification/footprint/ and ISP who accept certified Goodmail: http://www.goodmailsystems.com/partners/who_accepts.php

Certification doesn't guarantee delivery to the inbox. It's not being used everywhere the same exact way. Certain ISPs may give you near guaranteed inbox delivery (although they probably won't say it). Others will have it at as a major determination factor, with shades of grey between the two. You can't buy your way to a good sender reputation or good deliverability. Even if a company has gone through the certification program, if they mail a list (whether intentionally or not) that has bad results then they will be suspended from the program. Certification is an ongoing evaluation.

Certification/accreditation programs do not solve all email deliverability problems; it's about a combination of approaches. Authentication is the first baseline, this allows the industry to target and track the sender's performance. Then a reputation and (optionally) certification is assigned to this identifiable entity, with more and more ISPs then using that information to filter or flow the email to the right place.

9. Manual Whitelisting

Since certification whitelisting is not in widespread use in South Africa one cannot rely on automatic whitelisting (see point 8 above). It is sometimes necessary to take manual steps to be whitelisted with various ISP and Webmail providers:

- The first step is analysis of rejected mail delivery and identification of patterns where groups of emails to a specific ISP or Web Based Mail Provider are experiencing delivery problems.
- Once this has been determined the problem sources are ranked from largest to smallest number of rejections; and a contact list is generated to request whitelisting. Generally the contact details for the responsible person or department will be available on the company website.
- If the problem source is a local company the most effective means of contact is a telephone call to the correct person followed by written correspondence via email.
- Large international companies are not easily contactable by telephone or email. Many do however have application forms on their website for motivating to be whitelisted. These forms should be completed and submitted. For example one such international company is Yahoo, the link to their form is: http://help.yahoo.com/l/us/yahoo/mail/postmaster/bulkv2.html

Before whitelisting a sender the ISP or webmail system operator may want to know what type of messages you are trying to deliver to their users, and may require proof that you have received optin permission from the recipients. If the ISP repeatedly receives a high number of spam complaints whenever they deliver your mails, the operator may refuse to whitelist your domain or may even blacklist you on their system.

10. Build up your reputation slowly

When you are new to bulk mailing (and have no reputation) you need to be extra careful about what you send in order to allow a good track record to be built up for your commercial sending, particularly if you are not using an ESP. Initially, traffic being sent from a new IP address should be restricted to no more than a few hundred or a few thousand per hour. This figure can then be increased as the reputation score builds. Some ISP's have a stated policy whereby the volume of email that they will process per hour is a direct function of the reputation score that is associated with the originating IP address. Most email broadcast software now has the ability to 'throttle' broadcasts, i.e. to restrict the number of emails sent to X per hour. Throttling can also be applied for individual ISPs. If you are using an ESP, then they will be responsible for building and maintaining the reputation of their IP addresses.

On your first communication, send to addresses that you are confident will be active and engaging. If email addresses have been obtained from one or more data sources, or if it is possible to sort the addresses as a function of recency, then it makes a lot of sense to prioritise the broadcasting of the addresses that are least likely to complain or bounce back. So, if one data source uses passive single opt-in while another source uses double opt-in to collect its addresses, broadcast the double opt-in ones first. Similarly, addresses that have shown signs of life within the past 90 days are going to be more responsive than those that have been dormant for a year or more. Bear in mind that this is a best practice recommendation and not a legal requirement – although preferable to a single opt-in, a double opt-in is not required by law.

Conclusion:

Closing thoughts

Quality email marketing is about owning a direct communication channel that subscribers trust to a point where it can influence their buying decisions. Once a company implements an email marketing program their database and email newsletter become a direct communication channel that they can use regularly to drive sales and strengthen customer loyalty. To get and keep subscribers on a mailing list, the newsletter must provide value to its recipients on a regular basis (give in order to take).

There are still many companies whose email strategy is characterised by high frequency, low value and lack of segmentation. To really tap into the tremendous return on investment potential that leading email marketer's experience, your company will want to be regular, consistent and constantly improving its direct communications.

By choosing a good technology partner; following even the most basic best practices like welcome messages, efficient opt-out procedures, appropriate permission levels and value propositions for your mail programs and avoiding spam like behavior (unwanted or unsolicited commercial mailing) a company will achieve a good sender reputation and increases the success rates of its email marketing.

About this document and the authors

This document has been published by TouchBasePro, (a South Africa based Email Service Provider) in collaboration with Email Connection and the Direct Marketing Association of SA.

The purpose of this document is to help foster an understanding of the technical issues surrounding bulk email deliverability, and promote best practices for email marketing in South Africa.

Published date: 7 December 2010

Written by: Cordell Brewer, B.Eng Elec & M.EM IAM
(TouchBasePro – www.touchbasepro.com)

Edited by: Greg Phillips, B.Sc Hons Comp Sci & B.Sc IT
(TouchBasePro – www.touchbasepro.com)

Darryl Richard
(Email Connection – www.emc.co.za)

Brian M. Mdluli
(Direct Marketing Association of SA – www.dmasa.org)

References and further reading

1. Direct Marketing Association of United Kingdom (January 2010). DMA UK Deliverability White Paper Review. Report available for download at: http://www.dma.org.uk/_attachments/resources/5892_S4.pdf

2. Epsilon International (2009). Email Deliverability Guide for the Asia Pacific Region 2009. Report available for download at: http://www.epsilon.com/international/pdfs/Epsilon_Intl_Email_Deliverability_Guide_for_the_Asia_Pacific_Region_2009.pdf

3. Return Path Certification: Best Practice Guide http://www.returnpath.net/commercialsender/certification/lib/documents/RPC_BestPracticeGuide.pdf

4. Return Path Certification: RPC_Certified Level Standards and FAQs http://www.returnpath.net/commercialsender/certification/lib/documents/RPC_Certified%20Level%20Standards%20and%20FAQs.pdf

5. Introduction to SpamCop for recipients of spam reports. Accessed on 23/09/2010 on http://www.spamcop.net/reported.shtml

6. ReturnPath (2009). The Global Email Deliverability Benchmark Report, 2H 2009. Report available for download at: http://www.returnpath.net/downloads/resources/globaldeliverability2H2009.pdf

7. Return Path's Deliverability and Reputation Handbook (2010). Report available for download at: http://www.returnpath.net/downloads/resources/ukdeliverabilityhandbook.pdf

8. Forrester Research (2009). US Email Marketing Forecast, 2009 To 2014. Report available for download at: http://www.forrester.com/rb/Research/us_email_marketing_forecast,_2009_to_2014/q/id/53620/t/2

9. ReturnPath Resender Study. Report available for download at: http://www.returnpath.net/resources/archives/ResenderStudy_101206.pdf

10. Cisco IronPort Anti-Spam Datasheet. Document available for download at: http://www.ironport.com/pdf/ironport_anti-spam_datasheet.pdf

Think Outbox
Think TouchBasePro

To trial TouchBasePro for free visit
www.TouchBasePro.com
or contact sales on
+27 11 447 9716 / +27 10 500 0024

TouchBasePro

The simplest message distribution service