

# BRANCH COMMUNICATIONS LTD

## GETTING IN THE INBOX

Hello, I'm Mike Parry, Managing Director of IPT Services Division EmailBureau. To give you a little background I was involved in the launch of the first ASP email broadcast platform in the UK back in 1999 with a company called e2communications. When e2 was acquired by Bluestreak in May 2002 I left to set up EmailBureau with the backing and support of IPT.

EmailBureau entered the market in August 2002 with a different slant on the standard ASP model, offering a fully managed service direct to marketers. Over the last 3 years EmailBureau has grown to be one of the leading specialists in the marketplace managing campaigns for over 90 clients in 2005 and sending in excess of 780 million emails in the calendar year. It is this experience that has given the depth of knowledge against which we draw when it comes to email deliverability and have produced this white paper in collaboration with Branch Communications Ltd.

Email deliverability or "Getting in the Inbox" has become the key issue facing email marketers over the last year, and is becoming increasingly important as businesses are looking to squeeze even more profitability out of their marketing spend.

Why is getting in the inbox so difficult is a question I'm often asked and it's something that doesn't have a simple answer. Back in the good old days the ISP's, the Hotmails, Yahoo's AOL's etc, used to measure themselves on the number of emails they received against the number of emails they managed to deliver - and the more they put in the inbox the more pleased with themselves they were. Those halcyon days are gone forever and they've gone because of the proliferation of SPAM that is sent around the world. The war against SPAM is one that is being fought on a number of fronts but unfortunately we fight against a relatively devious and anonymous enemy. In the US the CAN SPAM act has cleaned up the amount of SPAM generated in those shores however, the SPAMMERS have just relocated their operations to locations in the world who are less legislative in the war and who also have good broadband infrastructures. According to Commtouch." –from August 2005: "Spam continues to flow from all regions of the globe. China (19 percent), South Korea (17 percent), and the U.S. (15 percent), continue as top sources for spam origination.

In Europe the European Community have tried to legislate against SPAM outlawing unsolicited messages sent to consumers. Although well meaning this legislation appears toothless as most businesses in the UK and Europe already adhere to best practice outlined by the email marketing council, which in itself is part of the DMA. So despite a couple of highly publicised cases in the US and a couple of jail sentences legislation has proved largely ineffective.

The war then needs to be fought by the ISP's, who have at least a couple of reasons to undertake the fight. To put things into perspective, MSN Hotmail receive and process well in excess of 100 billion emails per month and it filters over 65% of those as SPAM, in order to do this MSN have had to outsource their filtering process to a specialist who undertake the filtering of 30,000 emails per second. The cost of the bandwidth, the CPU and the employment of Brightmail all add up. In itself this might be reason enough to fight the war. However the ISP's are also fighting for users, commercially they make their money from eyeballs and the stickiest part of any ISP's site is the inbox. If they are not seen to be protecting their users from SPAM then eventually those users will get fed up with Free Herbal Viagra and Penis Enhancement emails or the latest cheap luxury Rolexes, and as every pair of eye balls stops coming to their site the ISP's revenue dwindles from all the impression based advertising.

So what are they doing about it? In general they filter based on 6 main criteria:

1. Copy & Content
2. Headers
3. Code
4. Load
5. Reputation Scoring

# BRANCH COMMUNICATIONS LTD

## GETTING IN THE INBOX

6. JMR or Junk Mail Reporting
7. Blacklists
8. Data Integrity

1. Copy - if your creative contains enough words and phrases that are currently perceived to be used by SPAMMERS then the filter process will kick in and the email will be put into the junk mail folder or worse still be deleted by the ISP. Content, if your creative is image heavy and the ISP's are currently receiving a lot of image heavy SPAM then, as above, the message gets filtered

2. Headers - ISP's are increasingly doing DNS look ups and / or SPF (Sender Policy Framework) and Sender ID checks. This is an area your email service provider is responsible for if you outsource your email broadcasting, and your IT department if you are an in-house email marketer. Your IP address and DNS records need to resolve correctly in order that you will not experience delivery issues as a result of this. Looking forward Yahoo are in the process of Beta testing their own product, developed in association with Cisco systems and called DKIM or domain key identified mail. This is effectively an encrypted version of the SPF with the sending mail server encrypting the IP address and the domain information and the receiving server un-encrypting it and then verifying it. Again this is the responsibility of your email service provider or IT team and is one of the key questions to ask when choosing a supplier or confirming the capabilities of your in-house system.

3. Code - Your HTML code needs to be validated to HTML 4.101 standard. As we build your creative we make sure we validate using the commercial version of HTML Validator Pro (<http://www.htmlvalidator.com/>).

4. Load - Most mail transfer agents open connections with the ISP's mail server and then try to force as many emails in as possible before the connection gets broken, this results in the ISP's filtering email out to the Junk Mail Folder. Using IronPorts top of the range mail transfer agent we open individual connections for each email, this subsequently means that we don't create a load issue with the ISP's. We also monitor their acceptance rate of connections and as a result of this when they slow down so do we, again lessening the chance of emails being filtered.

5. Reputation Scoring - ISP's and IP filter companies use IP address reputation scoring to ascertain whether you "look like a SPAMMER". They monitor complaints at [www.senderbase.com](http://www.senderbase.com) and if these complaints reach a threshold, normally 4 messages per million sent, then that impacts on your reputation as a sender. If you use an ASP solution ask your provider whether they allocate individual IP addresses per client or send off of a shared IP range, if you are sharing, your reputation will be effected by actions of other senders. If your Senderbase reputation is poor then you are less likely to get your emails delivered.

6. JMR or Junk Mail Reporting - If your data complains about you by hitting the 'this is SPAM button' in their browser window, the ISP puts an automatic and arbitrary block on your IP address filtering your email to the junk mail folder. If this happens, any email in the queue or any email sent in the next 48 hours will be affected.

7. Blacklists - All ISP's and almost all businesses use some form of third party as a barrier to entry. These third parties maintain a list of IP addresses from which they wont accept email as - in their opinion - email emanating from these IP addresses is considered SPAM. For the ease of maintenance most people outsource the list management to one of the major 3<sup>rd</sup> party IP Blacklist businesses. There are many of these of which 19 or so affect the UK market.

8. Data Integrity - The ISP's monitor the number of bounces they receive from an IP address, if the bounce number is disproportionate to the number of legitimate emails the assume that this IP address is involved in SPAMMING, they also monitor how an IP address reacts to

# BRANCH COMMUNICATIONS LTD

## GETTING IN THE INBOX

certain bounce notifications and if as a result of receiving what is considered a fatal bounce code an ISP still receives email from that IP address it, again, assumes the worst.

With these 8 key areas in mind, what can you - the marketer - do differently in order to ensure that you don't fall foul of these traps? The slightly flippant response as an email marketer would be to outsource these problems to an expert and rely on their skills, technology and knowledge to get you in the inbox such as Branch Communications Ltd. However, the reality is that some of this stuff is your responsibility and - while I would advise outsourcing - I would also advise consultation with the experts and implementing as many of the following recommendations as is commercially viable for you. The opportunity cost of non-delivery grows the bigger your database and the greater your email revenue and, subsequently, any decision to invest in the elements outlined below must be made in conjunction with a commercial input.

### 1. Copy & Content

Aren't these the same thing? Well no, copy relates to the words you use, while content relates to the balance between words and imagery. While there are no hard and fast rules on what that balance should be, an email where the copy outweighs the imagery by a 2-1 ratio is considered best practice. However, where the copy you use could be considered to be similar to that used by SPAMMERS, ie; if the use of gambling terms, pharmaceutical terms, financial services terms, talk of money and sexual references is unavoidable in your line of work, then testing the balance by turning copy areas into images and subsequently avoiding terms like 'consolidate debt' or 'free £50 bet' is advisable. How do you know what's considered bad today and what's not? Unfortunately, the only way is through testing and then running your messages through some form of SPAM scorer. There is some freeware available from SPAMASSASSIN which -although OK - is very difficult to integrate with most email applications whilst at the same time gives a limited score based only on the copy and content and not also on the hard-coded aspects of the email such as the 'from' and 'reply' paths or the message headers. Alternatively there are system agnostic commercial tools available, best known and most widely used in the UK is IPT's MessageCheck solution which can be found at [www.emailmonitor.co.uk](http://www.emailmonitor.co.uk) . What I would say at this point is that this is only one of the elements against which the ISP's are filtering so don't get to hung up on it if your emails in the inbox. Move on!

### 2. Headers

This is kind of techie. Actually its really techie! Quite dull, but massively important. As marketers, you only need to understand what the process is and make sure that your Email Service Provider or IT department (if you use your own technology infrastructure) know what they are doing. Learn enough from here to ask the right questions, and don't be fobbed off with non-specific answers. The importance of headers relates to two email verification processes, championed by MSN/Hotmail and Yahoo - two of the largest email address providers both Globally and in the UK. The verification processes are 'Sender ID' by Microsoft and 'DKIM' by Yahoo. Both have been developed with the help of industry partners and I make no apologies for reading the explanations of these systems direct from the relative websites.

### **Spoofting and Phishing Defined**

Email spoofing - the forging of another person's or company's email address to get users to trust and open a message - is one of the biggest challenges facing both the Internet community and anti-Spam technologists today. Without sender authentication, verification, and traceability, email providers can never know for certain if a message is legitimate or forged and will therefore have to continually make educated guesses on behalf of their users on what to deliver, what to block, and what to quarantine, in the pursuit of the best possible user experience.

# BRANCH COMMUNICATIONS LTD

## GETTING IN THE INBOX

### How Sender ID Works

Sender ID seeks to verify that every e-mail message originates from the Internet domain from which it claims to have been sent. This is accomplished by checking the address of the server sending the mail against a registered list of servers that the domain owner has authorized to send e-mail. This verification is automatically performed by the Internet service provider (ISP) or recipient's mail server *before* the e-mail message is delivered to the user. The result of the Sender ID check can be used as additional input into the filtering tasks already performed by the mail server. Once the sender has been authenticated, the mail server may consider past behaviors, traffic patterns, and sender reputation, as well as apply conventional content filters when determining whether to deliver mail to the recipient.

What is SPF?

The questions are

- A. Are we SPF and Sender ID compliant? It's a yes or no question, there's no grey area. If the answer is 'yes' – great - move on. If it's no, you need to dig further to find out why not and what's happening to make you compliant. If you're not SPF compliant you will not get in the inbox in MSN/Hotmail.

DomainKeys is a technology proposal that can bring black and white back to this decision process by giving email providers a mechanism for verifying both the domain of each email sender and the integrity of the messages sent (ie; that they were not altered during transit). And, once the domain can be verified, it can be compared to the domain used by the sender in the 'From' field of the message to detect forgeries. If it's a forgery, then it's Spam or fraud, and it can be dropped without impact to the user. If it's not a forgery, then the domain is known, and a persistent reputation profile can be established for that sending domain that can be tied into anti-Spam policy systems, shared between service providers, and even exposed to the user.

For well-known companies that commonly send transactional email to consumers, such as banks, utilities, and ecommerce services, the benefits of verification are more profound, as it can help them protect their users from "phishing attacks" - the fraudulent solicitation for account information, such as credit card numbers and passwords, by impersonating the domain and email content of a company to which users have entrusted the storage of these data. For these companies, protecting their users from fraud emails translates directly into user protection, user satisfaction, reduced customer care costs, and brand protection. For consumers, such as Yahoo! Mail users or a grandparent accessing email through a small market town in England, industry support for sender authentication technologies will mean that they can start trusting email again, and it can resume its role as one of the most powerful communication tools of our times. So the question re domain keys which is currently being beta tested is

- B. Are we prepared for Yahoo's domain keys? Again it's a yes or no answer. Yes is good - no involves drilling down to find out what plans are in place to make you compliant.

I hope you've got enough of an understanding from this to hold your own with your technology team be that internal or email service provider to get to the bottom of these issues.

# BRANCH COMMUNICATIONS LTD

## GETTING IN THE INBOX

### 3. Code

An estimated 9 out of 10 HTML emails are not W3C HTML compliant, which can cause rendering as well as delivery issues, particularly at MSN and Hotmail. One of the dirtiest tricks in a spammer's arsenal is invalid, broken, and malicious HTML code, used to obfuscate his payload. If you use HTML in your messages, make sure your code is error-free and follows W3C HTML guidelines.

There is some freeware available for validation, the best being the HTML validator provided by W3C at [www.w3c.org](http://www.w3c.org), however we use a commercial validator from <http://www.htmlvalidator.com/> which can be customised to be more suitable for email as email browsers render slightly differently from web browsers and can also have a problem with scripting. When building your HTML remember to avoid scripts such as ASP, JSP and Javascript.

Security risks due to script vulnerabilities in email browsers have increased over the years. The result is most scripts, such as JavaScript and VBScript, are stripped out of messages. Some email systems reject messages outright if scripting is detected. For greatest compatibility, avoid using scripts in messages. Instead, drive your readers to your Web site, where dynamic components are easily rendered.

### 4. Load

The ISP's are creaking under the shear volume of emails they receive, someone like MSN/Hotmail are receiving in excess of 30,000 emails per second on average. When this spikes they struggle to cope, there are then 2 coping mechanisms that kick in, one is queuing, the emails sit in a large queue waiting to be delivered and the other is filtering. The second relates to filtering, an under pressure ISP may lower its threshold in the filtering process to reduce the number of emails left in the queue. Alternatively if your technology is not state of the art and opening individual connections for each email you may experience filtering because of a bottleneck, ie; too many emails trying to get into an ISP from one server at any one time. For the gentlemen amongst you this is the online equivalent of not getting into a night club because you're with a group of mates. In order to combat this you need to slow down the rate of delivery. As an email service provider I am often asked what capacity can I send emails out and although it's an almost impossible question to answer accurately because of the variables within the email itself I always find myself answering based on capacity which is in excess of 10 million emails per day, the truth of the matter is that capacity should be slowed down to the lowest common denominator which is in effect the ISP's. I advise throttling your send, using a mail server that monitors its speed of connection and makes intelligent decisions based on the information it receives. If the ISP slows down then the attempted connection speed should automatically mimic that speed, basically allowing the ISP to receive the email in its most suitable timescales.

### 5. Reputation Scoring

How do you improve your reputation score? Firstly, don't share IP addresses. Secondly, make sure you offer a clear unsubscribe process. Thirdly, Explain to your data why they are receiving the email. Fourthly, Offer a monitor complaints email address, if the data can complain to you they are less likely to complain about you. Fifthly, Explain what you plan to do with the data clearly on collection. Sixthly, Keep your data clean. Seventhly, Use an accreditation service like Habeas, that's [www.habeas.com](http://www.habeas.com), or an email verification service like Bonded Sender, [www.bondedsender.com](http://www.bondedsender.com). My personal advice is to investigate bonded sender run by Return Path and using Trust-e's certification. The cost of the bond varies depending on the volume of email sent but should be weighed against the opportunity cost of non delivery.

# BRANCH COMMUNICATIONS LTD

## GETTING IN THE INBOX

### 6. JMR or Junk Mail Reporting

Does your email service provider or your IT department acquire the available Junk Mail Reports from MSN/ Hotmail and AOL and remove this data from mailing files in the same way you'd remove an unsubscribe. Hotmail and MSN have only made this information available in

the last few weeks and this is another step towards responsible emailing that your email service provider should be taking toward reducing the chances of being blocked. Holding suppression files like this and running them across your live file not only improves your direct relationship with the ISP's but also improves your reputation scoring.

### 7. Blacklists

Being on a Blacklist used to strike fear into Email Marketers hearts but there has been a shift in how these are being perceived by the ISP's and also how you as a marketer can get on or off of one. There are in excess of 50 IP blacklists currently circulating the internet. As you can imagine these are managed in a range of different ways, from the very responsible, SpamAssassin, Spam Haus, SpamCop etc to the less than professionally run, those who will remain nameless but who know who they are. Anyone at anytime can get added to a blacklist however, the responsible lists give you the opportunity to plead your case and prove you're a legitimate marketer and will remove your IP address from their list if you have followed the relevant legislations. The more professional lists also monitor the volume of email traffic sent down your IP address and if after a block has been automatically added to an IP address that IP ceases to send email, usually for 48 to 72 hours the block will automatically be lifted. The problem for marketers is how do they know they are on the list? There are 2 ways, firstly get a list of the blocking companies operating in your region, in the UK there are approximately 19, get the URL's for each of these companies and each of your IP addresses daily, a laborious task! Alternatively you can sign up to one of the commercially available tools from either IPT, [www.ipt-ltd.co.uk](http://www.ipt-ltd.co.uk) or return path, [www.returnpath.net](http://www.returnpath.net).

### 8. Data Integrity

Good data is at the heart of good direct marketing and that's never been truer than when discussing email marketing. Without good data much of the money invested in creating and broadcasting emails may be wasted. Data is a living thing constantly changing and it is those changes that you as a marketer need to take into consideration. ISP's look at numbers of bounces, therefore any validation or cleansing of your data will reduce those fatal bounce numbers. Run an email Hygiene program across the data like IPTs or Return Paths and remove any email addresses that don't conform to international email standards. Look for common typo's and this will help improve your ISP relations. Don't keep mailing fatal bounces, if the ISP's send back a bounce notification which is obviously fatal remove that address from your file. The cleaner your data the better chance you have of deliverability. Try and work with the ISP's rather than round them.

Email Deliverability or getting in the inbox is a minefield, what was good 2 years ago is irrelevant now, what you knew a year ago needs updating today. Don't rest on your laurels because you will find yourself falling behind your competition, always try to keep your finger on the pulse. Although email marketing is seen as relatively cheap form of communication the opportunity cost of non delivery can make it disproportionately expensive. If in doubt, outsource.

Thank you for listening, if you want any further advise please don't hesitate to contact me Mike Parry by email [mike.parry@ipt-ltd.co.uk](mailto:mike.parry@ipt-ltd.co.uk) or Branch Communications Ltd at [marketing@branchcommunications.co.uk](mailto:marketing@branchcommunications.co.uk)