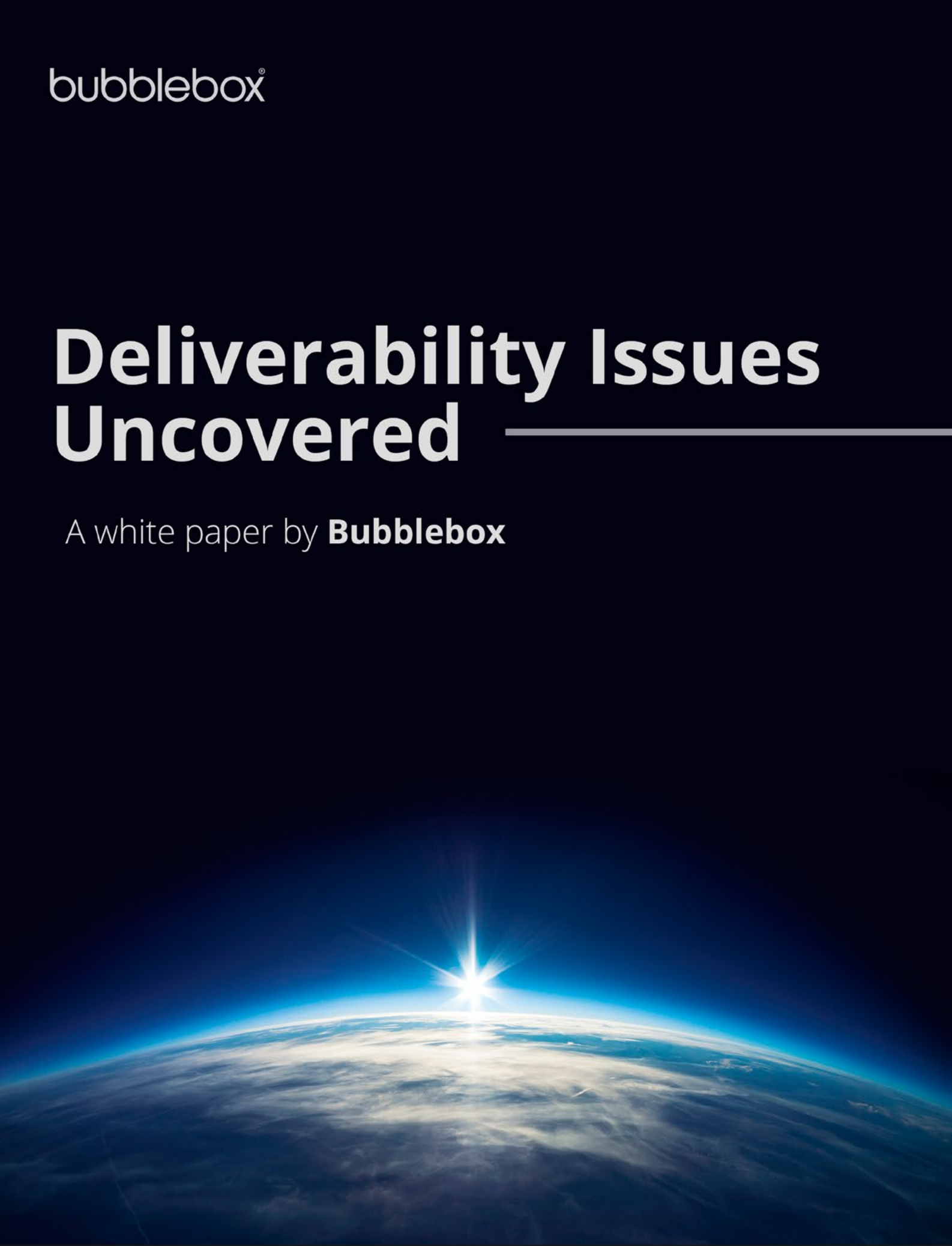
bubblebox®

Deliverability Issues Uncovered

A white paper by **Bubblebox**



We have a global reputation for implementing strategic solutions for our customers. We are Cross-Cloud experts with proficiency in Salesforce Sales, Marketing, Service and Community Clouds as well as Pardot - all delivered with incomparable customer service and a commitment to measurable results.

www.bubblebox.cloud | T: 888.247.8495

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

Purpose of Document

Ensuring that your subscribers receive the emails you've sent them, and have viewed them as intended, is essential to brand perception and usability. It is of course logical that if messages sent to prospects, customers and subscribers are relevant, timely and interesting, then conversion rates will increase. What is often forgotten is that these same logical practices and principles of sending relevant, timely and engaging emails has as a large of an influence on deliverability into a recipient's inbox as the technical factors Email Services Providers claim to resolve.

This document aims to outline the areas of deliverability that are essential to maintaining a high level of customer engagement and retention. This is not an exhaustive list as we are continually improving the service on behalf of our customers.

1. Server Factors

2. Creative Technical Factors

3. Frequency Factors

4. Human Factors

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

1. Server Factors

The following outlines areas whereby the Server side of email sending has a large impact on deliverability. This is particularly relevant if the company uses an in-house solution or a lower level Email Service Provider (ESP) that does not adhere to these best practice areas. These include the following:

- The IP reputation (the IP Address identifies a computer/server and emails have this identified within the email header).

- ISP's all maintain their own view of the reputation of an IP address therefore if the sender (ESP) has a history of SPAM email then it is highly likely to be blocked. IP Reputation is one of the most significant factors used by the major ISP's. Other companies may monitor IP reputations include SenderBase™ and SenderScore™, however the definition of a good IP reputation will differ to that of each ISP.

- SPF (Sender Policy Framework) – Provides authentication that the sending domain matches that of which is shown within the email header when the ISP received the email. ISP's use this confirmation as part of their scoring system – if an email does not carry an SFP then it will score poorly. Some ISP's such as Outlook.com will show 'sender not verified' if incorrect and as a result may not deliver the email at all.

- DKIM (Domainkeys Identified Mail) - Allows the receiving server to check if an email claimed to have come from a specific domain was in fact authorized by the domain owner. Similar to SPF, it is an email authentication method designed to detect email spoofing.

- In order to ensure that the ESP complies with SPF, a DNS TXT record is needed. This identifies the IP addresses that will send for a particular domain. When an email has a different domain to that used by the email sending server, then it may be deemed as SPAM. For this reason it is Best Practice to use an email domain that is either a subdomain of the main domain (e.g.mail.mydomain.com) or a completely new domain for email sending (e.g. @emailmydomain.com). If using an ESP, then the subdomain or the new domain DNS must be pointing towards the ESP's sending servers in order to ensure the correct authentication.

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

- **A & MX records**: An 'A' record is needed for click-throughs and open tracking. The 'MX' record is for emailing and is needed to verify sending IP address and for replies/bounces to be routed back to the server.

- **Reverse DNS**: Receiving mail servers take the senders IP address and reverse lookup to gain the domain name to check it corresponds to the sending domain. This is used for further authentication of sender.

- **SMTP HELO matching reverse DNS**: When mail is sent, the sending and receiving mail servers exchange their names. The senders name needs to be the same as the reverse DNS lookup –otherwise it will be seen as SPAM and be blocked.

- **IP Blocklists. Domain/SURBL:** Third parties maintain lists of IP addresses that are known to send SPAM, many of which are public. Destination mail servers check blocklists and use this for their scoring to accept or deny an incoming email.

- **ISP Whitelisting:** This is normally a technical relationship between those email senders who have a high reputation and the ISP.

- **Feedback loops, ISP's, SpamCop etc:** This is part of ISP programs to obtain information on who reports an email as spam. These feedback loops enable "safe-senders" to suppress email addresses from lists that have been reported as SPAM. The number of complaints an ISP receives from a given IP address or sending domain via a feedback loop is a major factor in the ISP's view on IP address reputation.

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

2. Creative Technical Factors

There are a number of items that senders should validate to ensure that their emails have the highest delivery success rate. The technical aspects of desig have a large influence on email deliverability. Below are some of the key guidelines that should be followed in order to ensure Best Practice is followed.

- **HTML validity**: If the HTML does not follow W3C standards, it will be more likely to be treated as SPAM. Further information about W3C standards can be found at http://www. w3.org.

- **Ratio of text to images**: It is important to ensure that the email is not constructed of images only. Retailers are notorious for this practice due to the visual advantages that images provide with regard to the products they sell. Unfortunately, SPAMers place text into images in order to hide it from content filters. Therefore, if there isn't much text in an email then this can appear to be more SPAM-like and the email is not delivered.

- **Dotted IP addresses:** You should never use dotted IP addresses within a link due to the perception that it is from a SPAMer or someone phishing for information. Always use domain or subdomain names. E.g. http://192.168.23.45/webpage.html - instead always use http://mydomain.com/webpage.html. A good example of this practice is that Outlook will block link clicks if any of the content within the links use dotted IP addresses. This is due to many phishing emails contain dotted IP addresses.

    - Links with SURBL listed domains: if your content contains links to websites which are on SURLB lists (SPAM URL real-time Block Lists) your emails will be considered more SPAM-like.

    - SPAM probability check: ensure that your ESP has the ability to gain not only a SPAM ASSASSIN scoring (of between 0-5) and also a content check to compare your email against the words most currently used by SPAMers "at that time".

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

3. Frequency Factors

Technical factors alone are not a guarantee that emails will be delivered and more importantly read by the recipient. One of the main aspects in assisting with deliverability is that of Frequency.

By sending emails too frequently, recipients may report your emails as SPAM. If too many recipients report you as SPAM rather than unsubscribe, then this will have an effect on the reputation of your IP address. Frequency control is dependent on the type of email and relevance. The optimum level will depend upon the types of messages you are trying to communicate with your customers and prospects.

It is imperative to ensure that content is targeted and relevant. Content sent to recipients whereby the information is not applicable or has low value will cause the recipients to treat the email as SPAM. Whilst this is common sense, lower end ESP providers all too often do not enable marketers to easily segment and profile their recipients in order to dynamically generate content according to previous recipient website, email or past purchase behavior. Consequently emails are often seen as cheap "fax by email" marketing – and consequently the company gains poor results leading to a conclusion that email is not an effective marketing tool.

Ensuring Content Congruence has a large impact on whether recipients see your email as being SPAM. You must ensure that the content sent is consistent with what the recipient was expecting after they signed up to your email. If it is not relevant, or looks dissimilar to the website they visited, then there is a high likelihood that it will be seen and treated as SPAM.

The email From Name identifies the name with which the recipient identifies you and is also equally important. If the user does not identify the email as being from someone they know or requested emails from, then they are likely to consider it to be SPAM.

Data purging inactive addresses: It is important to remove addresses that are not adding value to your campaigns. Not only does this save money when paying CPM rates, but also this reduces volumes seen by ISP's and reduces the number of recipients hitting Report as SPAM. In addition, many ISP's use "SPAM Traps" that are dormant email accounts. If too many of your emails reach these accounts, ISP's will assume that you do not manage your data hygiene and you are likely to be perceived as a SPAMer.

Data hygiene is a large part of ensuring a high deliverability rate. Senders with bounce rates of >10% will be flagged by ISP's and this will affect your IP reputation.

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

4. Human Factors

A pitfall of Email Marketing that many marketers fall into is believing that technology will resolve any deliverability issues. When selecting a technology, not only should all of the aforementioned be the "de-facto" in ensuring that deliverability is at its highest, but also there is a high level of knowledge, experience, and consultancy available. Below are just some of the many areas that users of Email Marketing technology should take heed of in ensuring the highest deliverability levels.

Clarity of sign-up: When subscribers decided that they wish to receive information from you then it should be clear and obvious as to how their email address will be treated/used.

Double opt-in: To avoid malicious signups it is Best Practice to ensure that the recipient is sent an email that they need to confirm by clicking on the link. Any email that is then entered and not verified will be excluded from the emailing. Another verification tool often used is CAPTCHA.

Consistency of branding: Whilst this does link back to Content Congruence, this is referring to the design aspect rather than the content the recipient is expecting to receive. Not only should the email look like the website or form that the recipient completed, but also the content must be in line with their expectations.

A clear unsubscribe: By placing this at the bottom of the email and providing a clear and simple unsubscribe process, you will likely avoid many recipients reporting you as SPAM rather than simply unsubscribing from your email list. In addition, through the provision of a Preference Page, recipient can also subscribe to emails and content that they do/do not wish to receive.

One clear way to improve deliverability is to invite recipients to "whitelist" your From Email Address. Include a link at the top and bottom of your email with whitelist instructions.

Include personal data to strengthen human authentication. For example, greet a recipient by name or include partial postcode/zip code! This is data that would have been gained from the subscriber through the signup process. Using this information within the content of the email will strengthen your reputation. Include a reminder as to why the email has been received and how and when it was requested.

Finally ensure that you provide your company details and how a recipient can contact you. This is not only Best Practice, but this is also a legal requirement.

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud

bubblebox®

About Bubblebox

Bubblebox® deploy Salesforce for Marketing services to leading global brands. We understand the need to execute marketing-led initiatives as it relates to Sales, Service, and Marketing Cloud deployments that drive customer success. We are Marketing Cloud Experts.

Copyright and Disclaimer

Contact Us

info@bubblebox.cloud

#1500 - 885 W Georgia St
Vancouver, **Canada**
V6C 3E8
Canada: +1 888 247 8495

Hamilton House, Mabledon Place
London, **United Kingdom**
WC1H 9BB
UK: +44 20 3409 4448

WEST COAST OFFICE
#101-1847 West Broadway
Vancouver, BC V6J 1Y5
+1 604 357 7194
info@bubblebox.cloud

EAST COAST OFFICE
555 King Street West
Toronto, ON M5V 1M1
+1 647 499 5955
info@bubblebox.cloud