PHX MUG – July ‘23

Unlocking Deliverability With Marketo Engage

July 07/12/2023

gnw consulting

A Data-Driven, Marketing Automation Agency

Raja Walia
Principal Consultant / Founder of GNW Consulting

13x Years Certified Marketo Expert
Certified Architect/Master
Bizible Specialization
SFDC Admin / Dynamics Admin

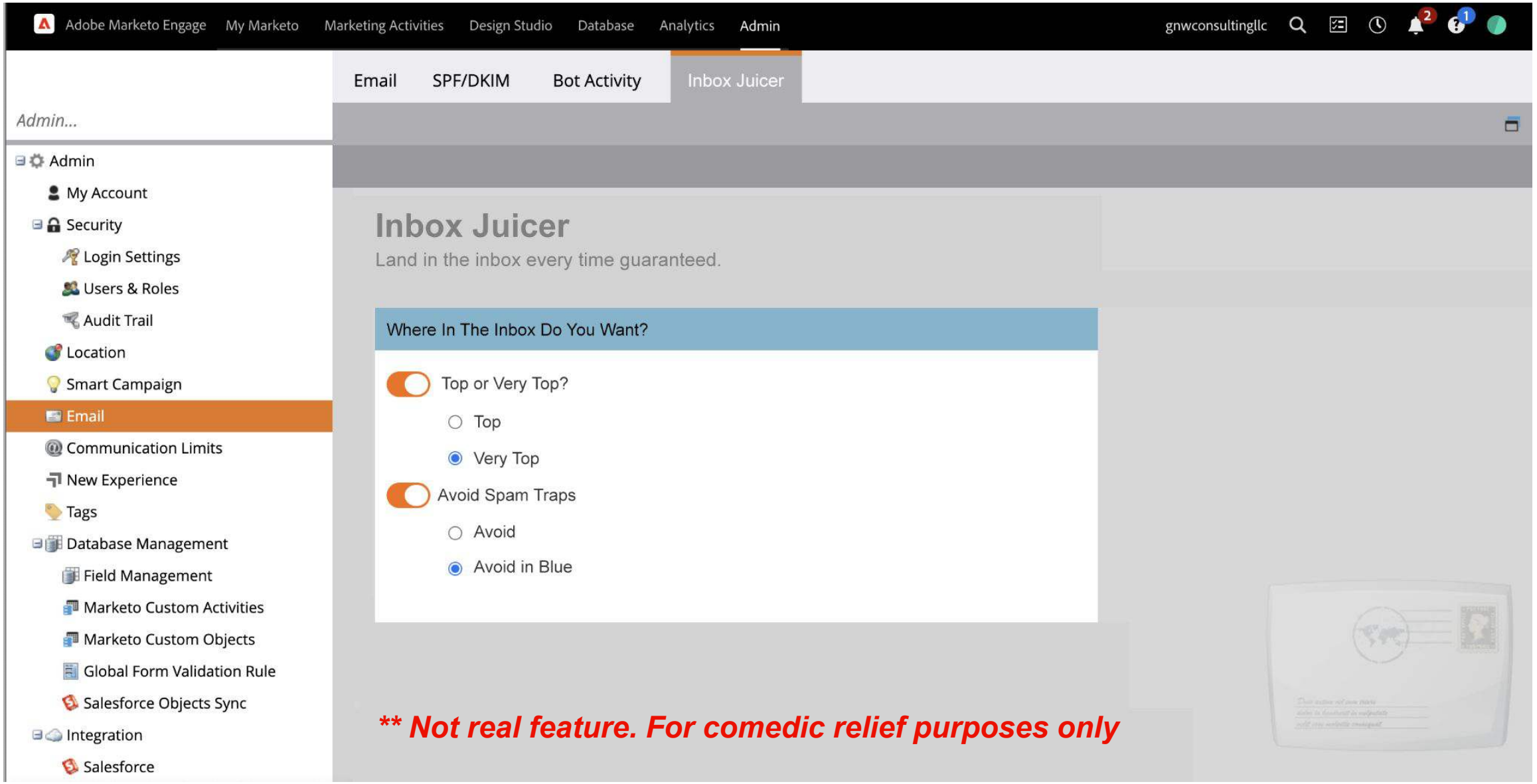
Akande Davis
Director Of Operations
GNW Consulting

1x Marketo Certified Master
3x Marketo Certified Expert

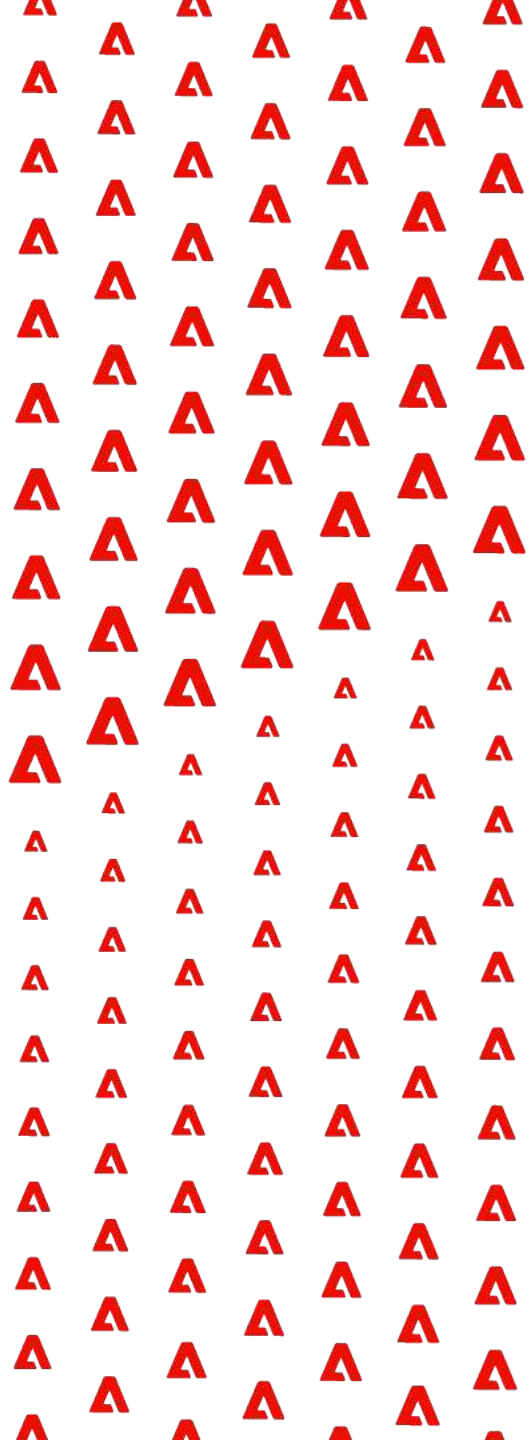
Agenda

- Inbox Juicer
- What Is Deliverability
  - Sender Policy Framework (SPF)
  - DomainKeys Identified Mail (DKIM)
  - Domain-Based Message Authentication Reporting and Conformance (DMARC)
  - Brand Indicators for Message Identification (BIMI)
- Deliverability Killers
  - Spam Traps
  - Blocklists
  - Database Cleanliness
- Cracking Email Deliverability in Marketo Engage
  - Bounce House
  - Non-responders
  - New Record Warm-up
- Tools (Free & Paid)

Inbox Juicer



What Is Deliverability?



Email Deliverability Is…

Email deliverability measures the success rate of your emails reaching subscribers' inboxes instead of being marked as spam and relegated to the junk folder. It directly impacts your business communication effectiveness, trust-building, and marketing success and at the end of the day, business revenue.

Your **Sender Reputation** is crucial and can be likened to building a reputable brand or personal identity. It's important to send emails that recipients genuinely want and engage with. When recipients consistently open, read, and interact with your messages, it signals to email providers that your emails are valued. Prioritizing recipient engagement and delivering compelling messages aligned with subscriber preferences is key.

Pillars of Deliverability

Sender Policy Framework (SPF):

When an email is sent, the recipient's mail server can check the SPF record published in the sender's domain DNS settings. The SPF record contains a list of approved IP addresses or domains that are authorized to send emails for that particular domain. If the sender's IP address matches one of the authorized IP addresses or domains listed in the SPF record, the email passes the SPF check and is considered authentic.

DomainKeys Identified Mail (DKIM):

DKIM works by adding a digital signature to the email headers of outgoing messages. This signature is generated using a private key associated with the sending domain. When the recipient's email server receives the email, it retrieves the public key from the sending domain's DNS records. The server then uses this public key to verify the signature in the email headers.

Domain-Based Message Authentication Reporting and Conformance (DMARC):

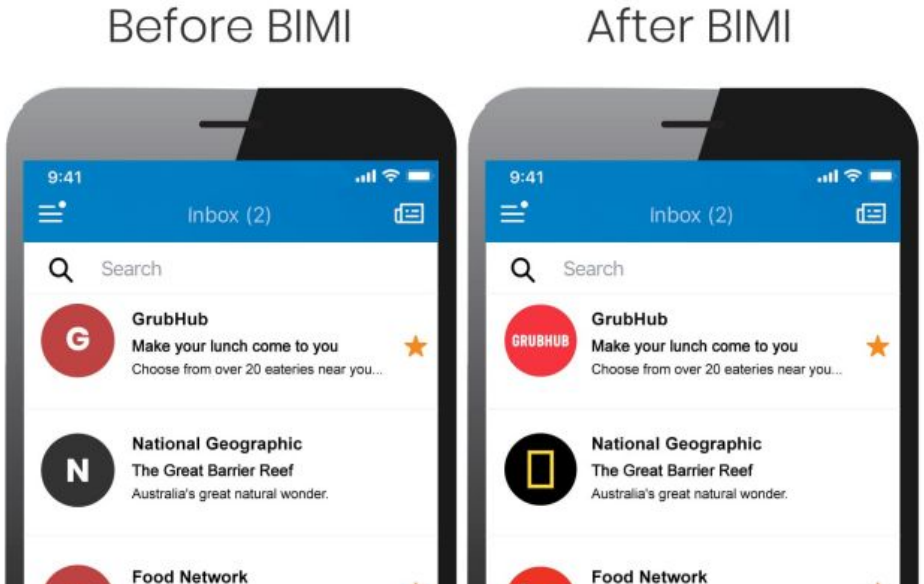
DMARC allows domain owners to publish policies in their DNS records, specifying how receiving email servers should handle emails that fail SPF and DKIM checks. These policies define the actions to be taken, such as monitoring, quarantine, or rejection of emails that do not meet the specified authentication requirements.

Pillars of Deliverability (Bonus)

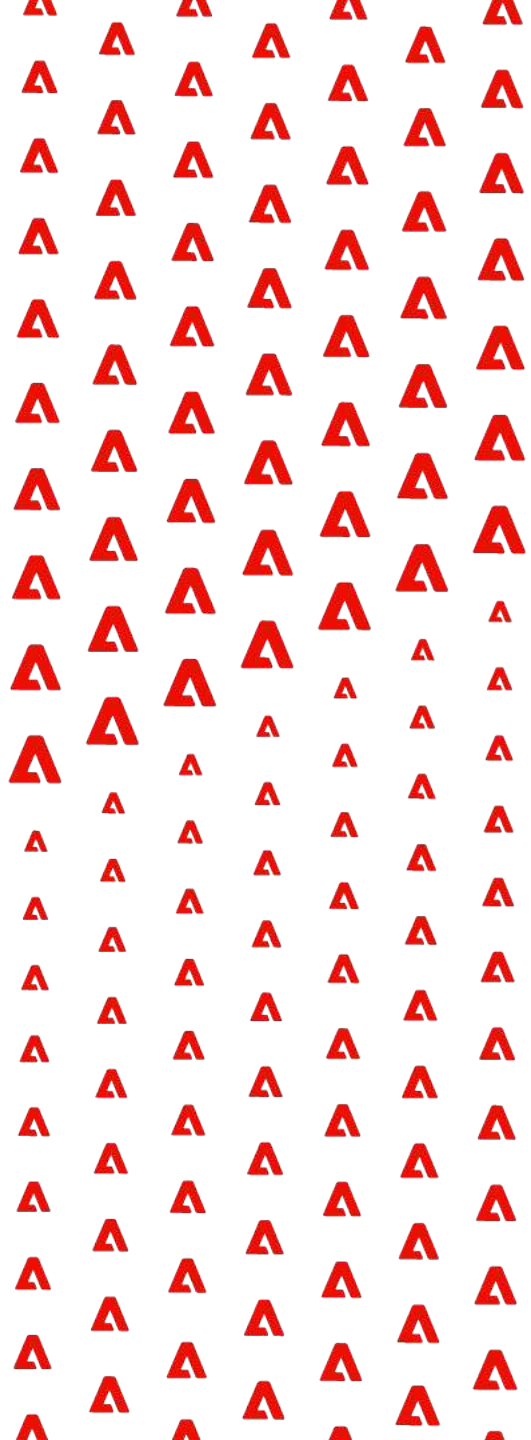
Brand Indicators for Message Identification (BIMI):

BIMI works in conjunction with other email authentication protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). It leverages these protocols to verify the authenticity of the sender's domain and the email message, ensuring that only legitimate senders can display their brand logo.

When an email is authenticated using DMARC and aligns with the BIMI policy, the recipient's email client fetches the brand's logo from a verified location specified in the DNS records of the sending domain. This logo is then displayed alongside the email in the recipient's inbox, providing a visual indication of the email's authenticity and associating it with the brand.



Deliverability Killers



Spam Traps

Pristine Traps: Pristine traps are email addresses that have never been associated with active mailboxes. They are intentionally published on websites to identify poor list acquisition practices or spammy senders. Pristine traps indicate serious issues with list acquisition since there is no legitimate way for these addresses to enter a list.

Recycled Traps: Recycled traps are email addresses or domains that were once active recipients but have become inactive (not accepting mail) for an extended period before being repurposed as traps. They highlight both poor acquisition practices and the failure to remove unengaged recipients from your list, posing a significant concern for list maintenance.

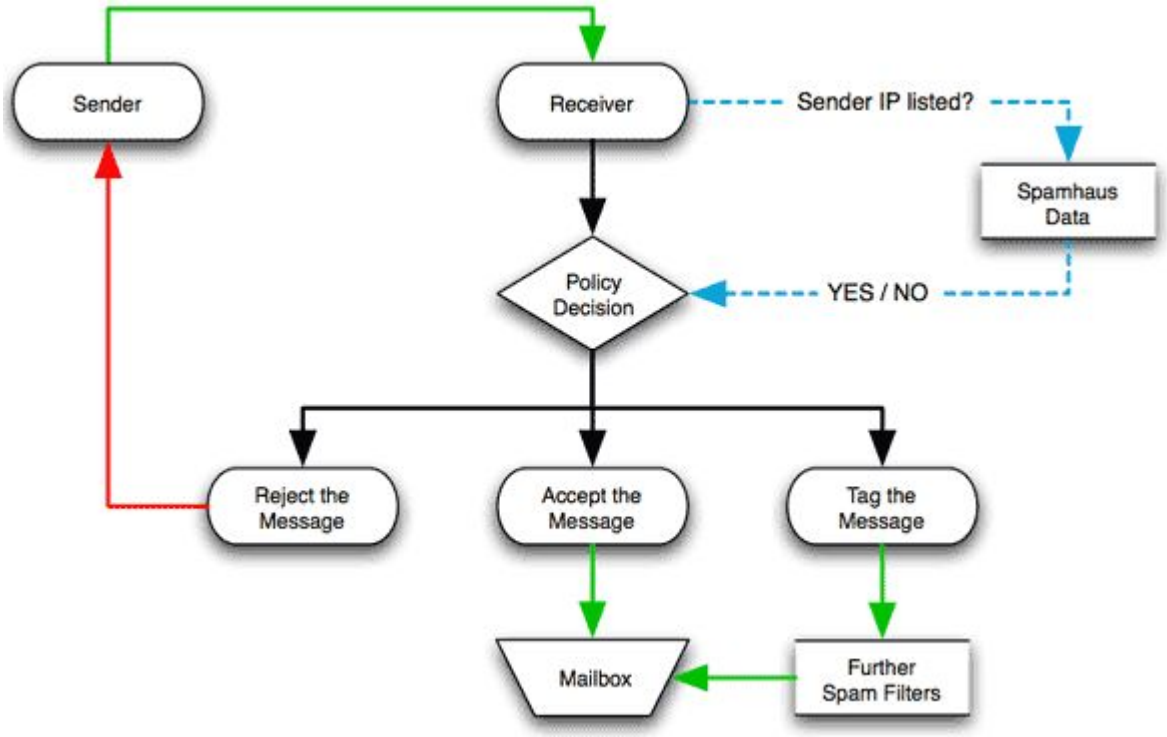
Parked Traps: These domains, while not technically traps, mimic their behavior and may point to list maintenance problems. Some domains are parked at registrars or monetization sites, like Namecheap or Above.com, while others are leased to commercial trap providers for their trap networks.

Typo Traps: Typo traps occur when individuals make errors while signing up for your mailings, resulting in incorrect email addresses. It is important to streamline and optimize your sign-up process to minimize these occurrences. While most typos are caused by human error, it's worth noting that some typo domains are owned by the Mailbox Provider.

Block Lists

Domain-Name System Based Blocklists (DNSBLs): A list of blocked sending domains

Real-Time Blocklist (RBLs): Catches offending IP addresses in real time



Senders can end up on blocklists for a number of reasons but it is primarily due to poor sending practices, sending to spam traps, email content etc.

When your email deliverability is affected due to being listed on a blocklist, you will typically receive a notification outlining the steps for potential removal. Blocklist providers often offer a self-service option where you can provide your contact information and explain the reason for the block. Some may provide a specific email address and subject line for your case.

Diagram of how blocklists operate courtesy of spamhaus.org

Database Cleanliness

Maintaining a clean database with active, engaged subscribers is an important part of maintaining your overall Email Deliverability. There are a few things to consider when looking at database health, including:

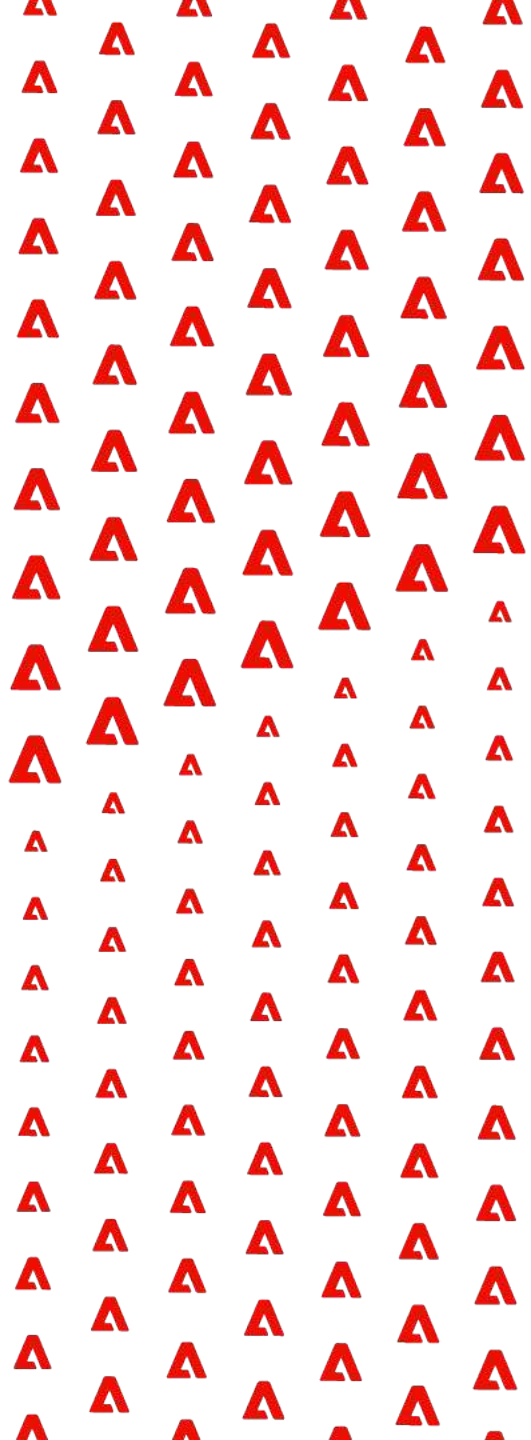
Old Email Addresses: What is the overall age of your current subscriber lists and how active/engaged are they with the content that is being sent out?

Inactive Recipients: If subscribers are not old or aged out, are they active and engaged with the emails that they are receiving?

Data Enrichment Tools: Are subscribers being enriched via a data enrichment tool with a high level of accuracy for subscriber details including email addresses?

Purchased Lists: Were subscribers acquired from a purchased list from a third party vendor/content syndication rather than voluntarily opting into your database?

Let’s Talk Marketo Engage

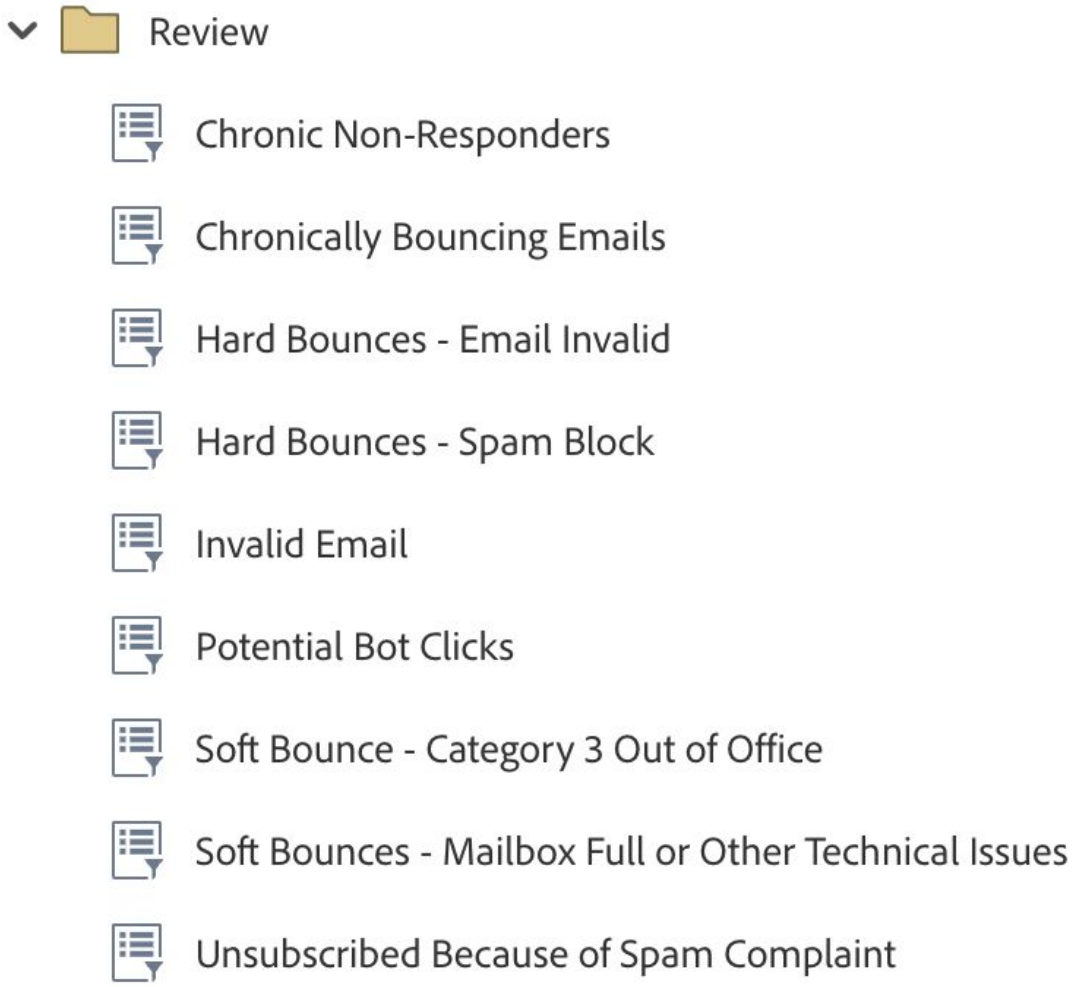


Our Bounce House Protocol

In every Marketo Engage instance we recommend creating a **Bounce House** Program. This Program leverages Smart Campaigns and Smart Lists to take care of **Bounces, Chronic Non-Responders, Invalid Emails, Bot Clicks,** and monitor **Unsubscribes due to Spam Complaints.**

Here is how we define each Smart List:

- **Chronic Non-responders** are Persons who received 5+ Emails ar did not Open or Click any of them in the last 2 months
- **Hard Bounces** are Persons who had a bounced email with a category 2 (Email Invalid) or category 1 (Spam Block)
- **Potential Bot Clicks** are Persons who exhibit Bot Click activity ***or*** received an Email and clicked a link in the Email but did not Open an Email or Visit the web page in the last 30 days
- **Soft Bounces** are Persons who soft bounce from an Email send with a category 3 and a subcategory of 3999 (Out of Office) a category 3 (excl. OOO) in the last 30 days
- **Unsubscribed because of Spam Complaint** is anyone who Unsubscribed and the reason is Customer complaint received from ISP



Right To Jail (Database) Jail

Our standard practice for Hard Bounces that are Spam or Email Invalid is immediate deletion, but for our **Chronic Non-responders**, **Chronic Soft Bounces** and **Potential Bot Clicks** we do something a bit different…

Persons that are impacting our Deliverability, but could be valid records, are marked as Marketing Suspended = True. While we may not want to purge from the Database, we do want to make sure they are valid. In these cases, those Person are added into our **Reactivation Program** as a last effort to capture them before completely purging them from the Database. Our **Reactivation Program** contains a few key elements:

1. We send out three text-based Emails over a one week period to records once they are added into the Program.
    a. The Email content is geared towards asking for *permission* to keep them in our Database and give them a heads up that they will be purged
    b. We use text-based Emails and keep the content as simple as possible
2. If a Person bounces on any of the Emails, they are added to the deletion bucket.
3. If a Person does not bounce but is unresponsive i.e. no Emails Opened, they are added to the deletion bucket.
4. If a Person does not Open but Clicks an Email, they are added to the deletion bucket.

Let’s Get You Warmed Up

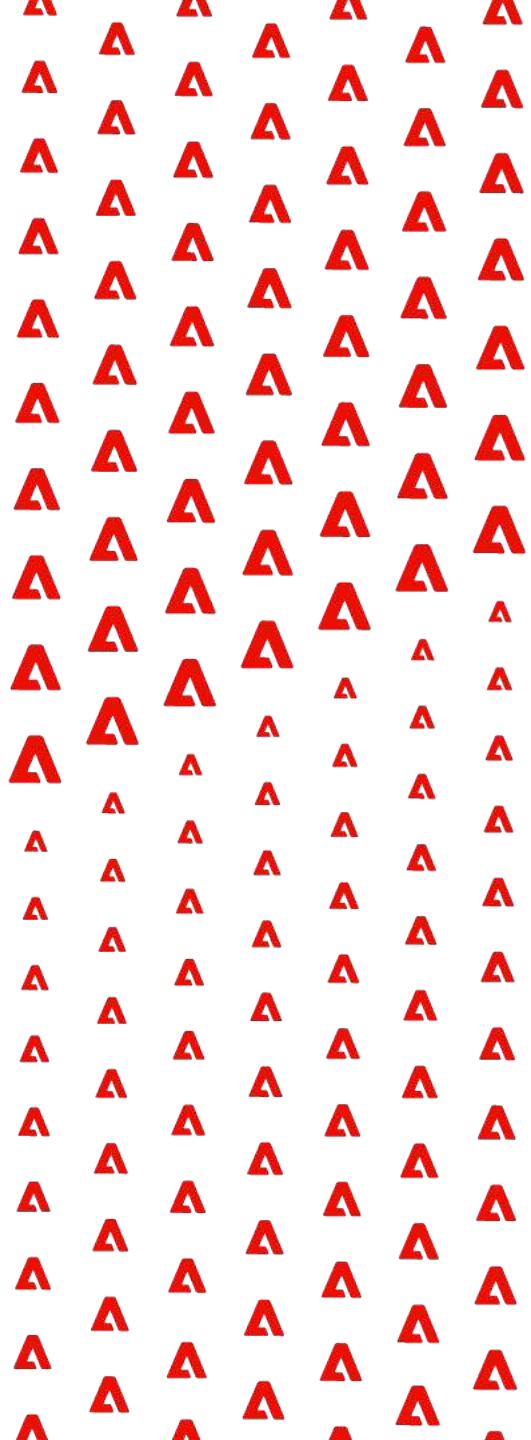
An element of Email marketing that is often overlooked, but is key in getting and maintaining great Email Deliverability, is the practice of warming up new Persons in the Database.

A *warm-up* period is a period where the Person will live on an exclusionary Smart List and receive Emails that are outside of the regular send cadence to demonstrate that they are valid, deliverable, and engaged. We recommend warm-up Emails to include token elements were possible (First Name, Company Name, etc.)

Examples of warm-up Emails include:

- **Welcome Emails**
- **Double Opt-in Confirmations** (most relevant for GDPR/CCPA)
- **Persona Surveys**
- **New Subscriber Offers/Rebates**
- **Text-based Emails** (usually sent from an LDR/Rep profile)
- **Whitelist Instructions**
- etc.

All The Tools



Leverage Marketo Engage Tools

Identify Problematic Audiences: We like to run **weekly Email Performance Report subscriptions** that drill down by **Lead Source, Industry,** or other relevant **Segmentation** to identify which audiences are the best or worst performing in terms of Email Deliverability. You can also use **domain specific Smart List rules** to only look at those records from Domains that are known to be offenders.

Track Offending Persons: Using **Smart List Subscriptions**, we can help easily identify which records are the cause of poor Email Deliverability and the ones being flagged as *spam, invalid domain, etc.* and allows the Admin to remove those records from sending and purge them.

Capture Bounce Details: With a combination of a Trigger based Smart Campaign and Custom Fields set to capture the Email Name {{trigger.Name}} that bounced, the Type of Bounce {{trigger.Trigger Name}} that it was and the Category of the Bounce {{trigger.Category}} admins can better track what Emails are leading to bounces which impact deliverability.

Dedicated IP Addresses: While a Dedicated IP Address does require a warming process, when done correctly, can yield incredibly high Deliverability rates when compared to shared IPs which can be impacted by other users leveraging the IP Addresses.

Leverage Marketo Engage Tools

Request Whitelisting: For specific Person segmentations that Marketo Engage is sending to on a regular basis, such as customers, you can request that they add the sender domain to an internal Allow list as well as the sender IP address. This will ensure that Emails make it to the inbox every time for that audience.

Everest Deliverability Tools: Within Marketo Engage, the Deliverability Tools provided by Everest can be a gamechanger when it comes to understanding inbox placement, Spam Traps hit, and even Email engagement beyond Opens and Clicks. Their robust set of tools work well with Marketo Engage to allow for a fuller picture of Email Deliverability performance.

Free Tools To Use

There are a number of free and freemium tools to use to help improve deliverability and troubleshoot how well your sending domain and IP address are performing. We recommend checking across multiple platforms to ensure that results are accurate:

- Google Postmaster Tools (Set this up if you haven't!)
- Microsoft SNDS (Set this up if you haven't!)
- Spamhaus.org Checker
- Sender Score
- MxtoolBox
- Barracuda Central

Next PHX MUG

- Let’s meet in person!
- **Recommendations on where we should host? Comment or email raja@gnwconsulting.com**


Adobe