The Essential Guide To *Deliverability*

Marigold's 2024 Guide to Deliverability

MARIGOLD™

Deliverability
The Unsung Hero of Email Marketing

Did you know that more than 347.3 billion emails are sent to subscribers across the globe, every day? Not all of those emails will reach inboxes - many of them either go to spam folders or are blocked.

In order to protect their users and networks, the Internet Service Providers (ISPs) generally cast a wide net. So if a message is flagged by an ISP filter to be spam, it's dead on arrival, never to see the light of the inbox. There are many layers to what and why an ISP categorizes an email message as spam. It's not just messages with malicious content or ones that a user didn't subscribe to. Legitimate marketing messages that subscribers want to receive can be flagged as spam too.

That's why it's essential for all email marketers to understand how to build and maintain strong deliverability.

Deliverability is the unsung hero of email marketing, ensuring emails reach their intended destination - subscribers' inboxes. Deliverability is determined by a host of factors, including the engagement of your subscribers, the content you send, and the quality of your lists. All together, these factors result in your sender reputation score and ultimately how the ISPs treat your email stream.

Although extremely important, deliverability can sometimes be considered a background player, and it's often not thought about - until there's a major issue.

To help demystify deliverability, Marigold's experts have created this essential guide. Read on to learn more about how deliverability works, how it impacts engagement, and the steps you can take to maintain a good sender reputation. Plus, we've also included best practices for list management, email content, and more.

Glossary of Terms

To understand deliverability is to begin with a vocabulary lesson.
Here's a breakdown of the key terms used when discussing deliverability:

BOUNCE

When an email is undeliverable, it bounces, which can fall into two categories:

Soft Bounce:
These occur when the ISP is blocking your email due to reputation issues or because of something temporary, like a full inbox or a down server. If you see a major spike in soft bounces at any ISP, you should address it immediately. Subscribers who have soft bounced are still valid and should be included in your next send.

Hard Bounce:
These occur when you send a message to a non-existent or invalid email address — think typos or a deactivated account. This is a permanent failure, and a metric that impacts sender reputation, so these email addresses should be removed from your list ASAP.

DELIVERED

A message is considered delivered when the ISP has successfully accepted the message. It's important to note that this doesn't equate to the message being delivered to the inbox.

DOMAIN

Referring to the locations of servers and devices connected to the Internet, domain names can represent various IP addresses and come after @ in an email address.

DOMAIN NAME SYSTEM (DNS)

This system maps a human-friendly domain name into a server IP address, almost like a telephone book. An MX type DNS record specifies where mail destined for a particular domain name should be sent. A TXT type DNS is used to contextualize information about the domain for authentication purposes.

CONTINUED

Glossary of Terms

EMAIL SERVICE PROVIDER (ESP)
The platform from which your emails are sent from - think our suite of Marigold email solutions.

FEEDBACK LOOP
For the ISPs (see definition below) that offer this service, feedback loops allow senders to receive a report every time someone marks their email as spam or junk, helping them identify issues early.

INBOX PLACEMENT RATE
When mail is accepted into an ISP's network, this figure refers to how many messages are delivered to the inbox. Please note this metric is not provided by the ISPs so to determine inbox placement it's important to look at a number of different data points, which layered together can help determine inbox placement.

INTERNET PROTOCOL (IP)
A number assigned to any device that's connected to the Internet, your IP address is how the ISPs identify you and your server.

INTERNET SERVICE PROVIDER
Think Gmail, Hotmail, AOL, Yahoo!, Verizon,Comcast and AT&T.

SENDER REPUTATION
This is the score tied to you as an email sender, which dictates the majority of email filtering. We'll cover this more in depth later in this guide.

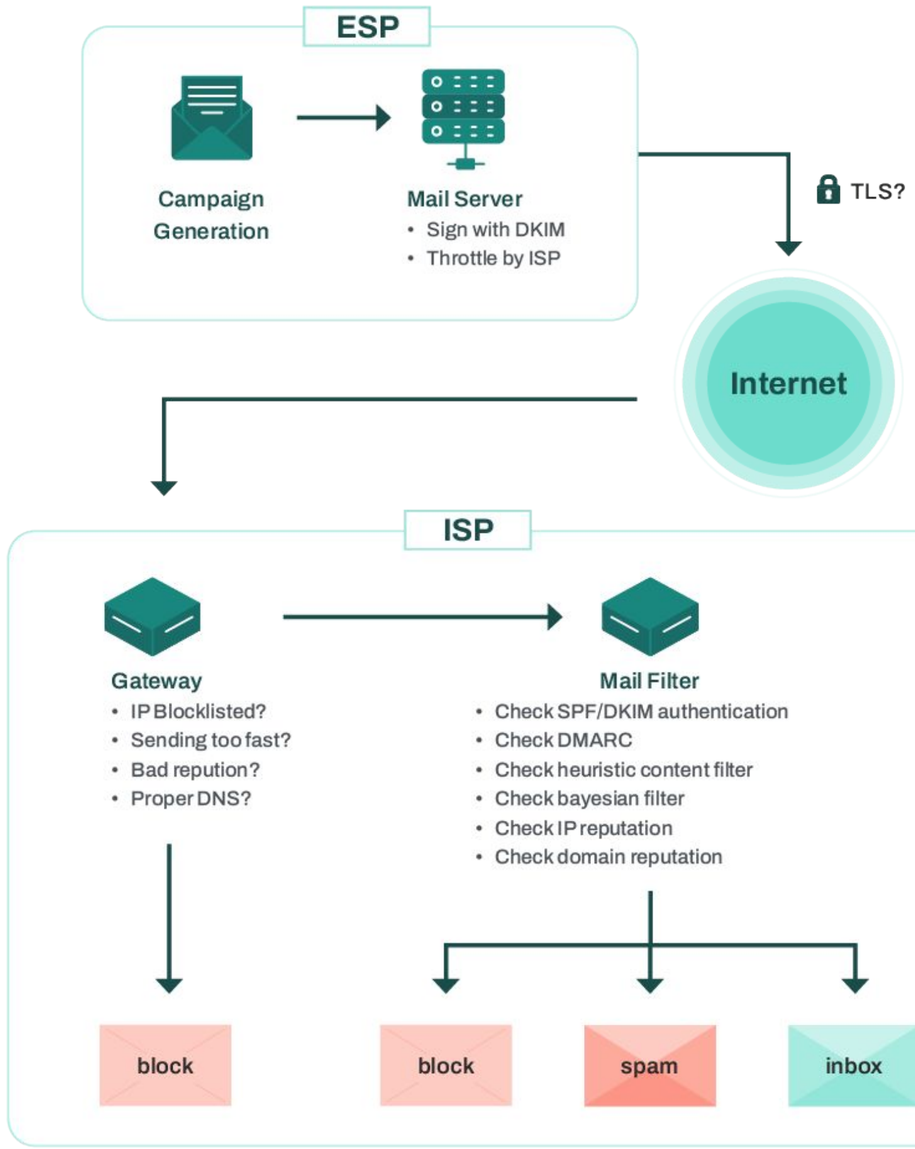
SUBDOMAIN
This is an extension of a brand's web domain, usually email.brand.com. Typically used for a brand's marketing emails, subdomains are often seen in the "from" address.

The Complex Path to the *Inbox*

Now that you've had that vocabulary lesson, let's get into how deliverability works.

Once you press send on your ESP's platform, the email goes into a queue to be delivered to the ISPs. The ISPs then accept the mail as fast as possible, on a "first come, first serve" basis. This depends on the domain name in the "To" field, for which DNS is used to identify the recipient's address. Next, the ISPs mail filters will check SPF and DKIM authentication (see 'Authentication for Email Delivery in 2024 and Beyond' section of this guide for definitions), the email's header and content, blocklists, and sender/IP/domain reputation. The results of these checks determine whether the ISP's network will accept the email and deliver it to the recipient's inbox or send it to the junk folder.

Though it may only take a few seconds, every email takes a complex journey to the inbox. Here's what it looks like.



Sender *Reputation* & Ability to Inbox

Each ISP uses thousands of different signals to determine sender reputation. An easy way to improve your sender reputation is to ensure you are sending to good quality subscribers, encourage and promote subscriber engagement, and get fewer Spam votes. It's important to note that sender reputation is determined on a rolling basis and is dynamic - so you shouldn't take a "set it and forget it" approach.

Sender reputation indicates how trustworthy an email sender is and dictates whether mail is:

01 **Placed to the inbox**

02 **Placed to the Junk Folder**

03 **Blocked and not delivered at all**

SENDER REPUTATION & ABILITY TO INBOX

The Four Main Drivers of *Sender Reputation*

1) SUBSCRIBER ENGAGEMENT

Send emails that your recipients will love. When your subscribers engage with your email by opening and reading the message, this sends a positive signal to the ISPs that determine your sender reputation.

- Keep an eye on your subject lines, creative, and send cadence to see what resonates and engages your audience. A/B testing elements is a great way to pulse check what your subscribers respond to the most.

- When you notice subscribers not engaging with your email, add them to a suppression list.

2) SUBSCRIBER COMPLAINTS

Any time a recipient hits the Spam button, it sends a negative signal to the ISPs. To reduce subscribers complaining, we recommend that you:

- Have explicit permission and voluntary opt-in. This ensures your emails are expected and wanted by your audience. We also suggest being transparent about when and what type of content your subscribers will receive. For example, if they've signed up for a weekly content newsletter - be sure to stick to that cadence and don't start sending daily sales offers.

- Check out our blog post **7 tips to reduce spam complaints** to learn how to keep your spam complaint rate well below Google and Yahoo's enforced 0.3% threshold. Our team of deliverability experts are committed to helping organizations target a spam complaint rate of below 0.1%, a level that all but eliminates the possibility of complaints that may create deliverability issues.

SENDER REPUTATION & ABILITY TO INBOX

The Four Main Drivers of *Sender Reputation*

3) INVALID USERS (HARD BOUNCES)

Sending to a high percentage of invalid subscribers is a negative signal to the ISPs. You'll likely always have a small number of hard bounces on campaigns since email addresses age out, but they shouldn't exceed 1%. Healthy senders are well below 0.1% so any spike even if not all the way to 1% can be problematic.

- Healthy email address collection paired with good sending practices should never result in a high hard bounce rate.

4) SPAM TRAPS

These are valid email addresses that don't belong to an active user, and they're used to identify senders with poor data quality practices as well as spammers. Mailbox providers, filtering companies, and blocklist administrators create and manage spam trap networks to monitor email received by spam trap email addresses. Spam traps can be classified in two ways:

- **Recycled Spam Trap -** These are email addresses that belonged to a person at some point but have since been abandoned or retired. After a certain amount of time during which the ISP would have sent out a user unknown error or hard bounce, the email address is reactivated and turned into a trap. These types of email addresses are typically present in stale lists that have not been mailed to in a long time and/or in senders' lists that have not had their hygiene maintained.

- **Honeypot (Pristine) Spam Trap -** These are email addresses that have never been given out or used for marketing or any other purpose. Since they aren't owned by live subscribers, the sole function of these email addresses is to catch senders and are often hidden on websites to be scraped or harvested. Any emails sent to these addresses are considered Spam.

Domain Reputation and *IP* Reputation

Both Domain Reputation and IP Reputation affect your overall Sender Reputation and ability to Inbox.

IP reputation is still important, but domain reputation has overshadowed it and tends to be the main driver for Inbox vs Junk Folder. The onus of following best practices and maintaining a healthy sender reputation is on each and every mailstream, whether you are on dedicated IPs or shared IPs.

This also means that domain warming is just as important as IP warming. The ISPs are sensitive to send volume and send cadence on cold IPs and cold domains. So, you'll need to follow a ramp up plan when mailing from a new dedicated IP or a new domain even if you're sending from warm IPs. So while IP reputation is easier to maintain, domain reputation has the majority of influence on inboxing.

Authentication for Email Delivery in 2024 and Beyond

ESPs have been holding their customers to a set of best practices for many years. These best practices are a culmination of known standards that various mailbox and RBL (Realtime Block List) providers have shared with senders. ESPs have largely enforced these best practices in AUP/Anti-Spam policies and have done the legwork on ensuring clients are using authentication.

However, on February 1st, 2024, Gmail and Yahoo introduced a set of new standards and requirements that all email bulk senders must follow. Failure to follow the new guidelines will result in your emails being rejected and not delivered. These new standards are being introduced as an effort to protect Gmail and Yahoo users from malicious emails and to try and stamp out identity theft via email and malware distribution.

The new standards are, for the most part, what ESPs have been recommending as best practices, so senders who have followed best practices are in very good shape for the changes. These new requirements can be grouped into three key categories:

- **Authenticate your email**
- **Make unsubscribing easier**
- **Stay below a spam threshold of 0.3%**

After evaluating the traffic passing through their networks, ISPs found that the vast majority of low-end spam is unauthenticated. By making authentication mandatory, ISPs can better filter and protect users' inboxes. DMARC is a policy that the domain owners publish in their DNS that instructs receivers of mail what to do with mail that claims to be from their domain but isn't authenticated to be from their domain. This is a powerful tool receivers can use to stop many streams of mail abuse. ISPs also want to make it easier for users to stop receiving unwanted email. Making it hard for users to unsubscribe goes against the best practices the ISPs have been promoting, and the new requirements from Gmail and Yahoo will make following best practices in this area mandatory.

What exactly is the goal of authentication?

It aims to prove two main things:

1) an email was sent by the organization that claims to have sent it and
2) the message hasn't been altered in transit.

Authentication for Email Delivery in 2024 and Beyond

Here are some helpful terms to understand when referring to authentication:

DKIM (Domain Key Identified Mail)

A method of using public and private keys to digitally sign the content of a message before it is sent. The receiver of the mail can calculate if the content of the message has changed based on the original digital signature added to the message. This gives mailbox providers the ability to say a message is the same message that was originally sent and nothing about it has been modified. The owner of the domain that is sending the message has the private key which actually sends the message so a message signature will be unique for that domain. Receivers are able to assign reputation based on the quality of email seen from that domain.

SPF (Sender Policy Framework)

A method for the owner of a domain to list resources (IP addresses) that are allowed to send email for that domain. When an email is received, the receiver can check DNS to see if the IP address the mail was sent from is listed in the domain owner's list of IP addresses allowed to send mail for their domain.

DMARC (Domain Message Authentication Reporting & Conformance)

A policy that uses the results of DKIM and/or SPF. The policy the domain owner tells the receiver of mail what to do with mail that is using their domain but doesn't pass authentication. DMARC can get nuanced and complicated based on the options that are implemented, but at its core, it is a policy the owner of the domain can use to announce what to do with messages from someone who is spoofing their domain. DMARC implementation needs to be done by someone experienced - if a DMARC policy is added without proper due diligence, it could impact that domain's ability to send mail.

Google and Yahoo's enforced requirements are just the beginning, with more and more ISPs moving towards a world of "No Auth, No Entry" - meaning they'll require everyone to properly authenticate their mail.

Domain reputation is going to become the primary driver of mail performance, which will necessitate senders taking a look at their practices and strategies to ensure they are sending timely, relevant, and expected mail to people who have asked to receive it.

Looking at *List Management*

List Health is integral to sender reputations. The main drivers of sender reputation (subscriber engagement, spam complaints, invalid users and spam traps) detailed above all rely on both healthy collection and list maintenance.

Consent and Collection

How you gain consent and data from your subscribers has a dramatic impact on your list quality. Our tips on healthy collection are:

- Users should give explicit permission to be emailed
- Make sure you're clear and obvious to subscribers about why and how their email address will be used
- Don't bury consent in your privacy policy
- Don't use a pre-checked checkbox. If subscribers really want to be on your list, they will take the time needed to tick the box
- Don't force anyone to give their email address or subscribe in order to browse your website
- Secure your opt-in page using Google reCAPTCHA to prevent BOT activity

CONTINUED

Looking at *List Management*

List Maintenance

Since audience engagement is a significant driver of sender reputation, it's important to remove those who aren't engaging. There are two groups of users to pay attention to:

1. **Subscribers who sign up and don't ever engage**
   The majority of engagement comes from new signups. If a user has signed up and doesn't engage with your emails within the first 30 days, it's very unlikely this user will become an active and engaged subscriber. They may also not even be a real user.

2. **Subscribers who have not engaged for some time**
   When a subscriber stops engaging with your emails, you should eventually remove them from your lists. We recommend contacting subscribers who have not engaged within the last year (in some cases, keep it to the last 9 months) with a re-engagement campaign - perhaps offer them an exclusive deal or content as an incentive. If they continue to not engage, we suggest removing them from your list or adding them to a suppression list.

Non-Human Interactions

You've likely started hearing more and more about non-human interactions. To understand how to combat them, it helps first to understand their definitions and what problems they can cause.

NHIs can present multiple problems for email senders. BOTs add poor quality email addresses that can include spam traps, list bombing addresses, and other malicious signups that either hard bounce or remain valid but don't engage. As outlined in previous sections of this guide, both hard bounces and non-engaging emails can negatively impact sender reputation. Interaction from NHIs – like MPP makes a potentially disengaged and/or poor quality address look active from a reporting standpoint and often leads to it continuing to be emailed even when it's not a good quality address.

To combat BOTs, keep an eye out for unusual spikes or certain patterns/variations in sign ups, which can signal that something isn't quite right. And be sure to add Google reCAPTCHA to all sign up pages.

There's no way to proactively identify and remediate NHI behavior, but you can use Marigold's offerings to get more accurate reporting. This will allow you to identify and target subscribers more accurately based on real user behavior rather than NHI actions.

BOTS

Automated programs that are able to sign up email addresses to non-secure signup pages. This is a tool commonly used to flood an end user's email box so that the account becomes unreachable. There are many reasons why someone might use BOTs - one is to flood an inbox so that the user can't get legitimate mail that might alert them of a credit card or banking fraud. This behavior is malicious, and it's extremely important to ensure your opt-in pages are secured from this type of activity.

NON-HUMAN INTERACTIONS (NHIs)

A BOT or software program that takes programmatic action that can't be distinguished from a human interaction. These interactions may impact the performance analysis and reporting of an individual message or email campaigns. Many NHIs are due to anti-spam software scanning messages to see if they have any malicious links or point to dangerous content - like websites that host malware or phishing pages. To ensure that security scanning isn't circumvented by bad actors, these link scanning patterns aren't obvious but are effective.

MAIL PRIVACY PROTECTION (MPP)

This is a specific type of NHI behavior included in Apple's software that results in a click on all links within a message.

Deliverability *Best Practices*

Here are some best practices across content, permission practices, and monitoring which can help improve your deliverability:

Content

While deliverability largely happens behind the scenes, content of your message also factors into whether or not your messages will hit recipients' inboxes.

- **Make sure your HTML is compliant** with the W3C (World Wide Web Consortium), the internet's main standards organization. Check out their very helpful validator tool as a starting point.

- **Avoid JavaScript** in the message body. Since JavaScript isn't naturally compatible with email, it may not load properly.

- **Create a mix between HTML and text** rather than using one giant image with text on it.

- **Use a consistent From address**, one that helps recipients easily identify your brand.

- **Never use link shorteners other than your own.** Branded short links like Goo.gl are popular with spammers looking to send people toward malware and viruses. As a result, short links aren't highly regarded by ISPs and are often blocklisted.

- **Avoid images with shared domains.** They're often used by thousands of senders, and if one of them is on a blocklist it can impact everyone else.

- **Optimize your subject lines** for both engagement and delivery. For tips on how to start A/B testing and more, check out our **Ultimate Guide to A/B & Multivariate Testing: Marketing Emails**.

- **Add alt text to every image.**

- **Use responsive design** to optimize how recipients view your email from any device.

- **Include your business name and address** in the footer of your email.

- **Ensure you have a functioning and easy-to-spot unsubscribe link.** Use of a preference center can help retail users.

Permission Practices

Not all permission practices were created equally. How users are collected in the first place has an impact on your data quality. Once you collect subscribers, you should make sure to keep an audit trail of permission - something global regulations increasingly require.

Explicit Opt-Ins

Before sending any emails, you're legally required to ask for opt-in permission. This involves a subscriber actively confirming they want to receive your emails. We recommend using a signup form - our Marigold products having features and functionality that make setting up a signup form easy. Remember, it's essential to preserve evidence that your audience has opted-in to receive emails.

Double Opt-Ins or Confirmed Opt-Ins

Are even better. This is a second step or email sent after the initial opt-in is given, and involves your audience confirming for a second time their opt-in, meaning there's a higher chance of weeding out any accidental signups. Double (or Confirmed) opt-ins also promote a great customer experience, ensuring your relationship with subscribers starts off on the right foot.

The Gray Area

An example of this may be when a customer fills out a form to download content or register for an event. Technically you have permission to email the customer under most jurisdictions, but they didn't necessarily sign up to receive all of your emails. As a result, implicit opt-ins can risk your messages making their way to subscribers' junk folders.

Sweepstakes and competitions represent another signup tactic to be wary of.
These are an effective way to grow your email list, but they can also be risky. They don't always disclose that while you can win a prize, you'll be subscribed to a brand's mailing list. One safe practice may be to email these subscribers separately to confirm opt-in and to ensure your list remains healthy and engaged. Remove anyone who doesn't engage from this source sooner than you would from a direct signup source.

Permission Practices

Things You Should Never Do:

Don’t use pre-checked boxes on your sign up forms.

If users want to receive your email, they will take the time to check the box and sign up. Collecting users who want to receive your email will result in stronger engagement and fewer complaints. We recommend consulting with legal counsel if you have questions about consent under applicable laws and regulations.

Be cautious with co-registration.

When a consumer registers for an offer, co-registration allows them to simultaneously opt-in to multiple offers. As a result, their data will be transferred to both advertisers on the form. However, they may not necessarily want to be contacted by both.

Don’t use purchased lists or email appending.

On the opposite end of the spectrum from explicit opt-ins are email appending and purchased lists. Also known as e-appending, the former involves obtaining email addresses by matching known customer data against a vendor’s database. The latter refers to lists purchased, filled with people who haven’t actually subscribed to receive emails. Those users may immediately flag sent messages as spam on principle. You should always use your own lists.

Monitoring Deliverability

Keeping an eye on your deliverability rate and bounces, monitoring your open rate, and using solutions such as Gmail's Postmaster Tools will help you proactively identify any potentially problematic areas.

Deliverability Rate and Bounces

Increased hard bounces will count negatively towards your sender reputation. Hard bounce causes may include forgetting a suppression list, poor quality acquisition sources, and/or BOT signups. Once you identify an issue, be sure to correct it immediately. Increased soft bounces usually mean your mail is being blocked by the ISPs. You'll need to investigate to determine what caused the block, escalate for removal, and implement best practices to make sure it doesn't happen again.

Open Rates

ISPs don't provide insight into whether mail was delivered to a recipient's inbox or junk folder, so open rates are the best indicator of a potential inboxing issue. Watch for any significant dips in open rate across all major ISPs. A notable dip at one ISP without a dip at the others is a strong indicator of an inboxing issue you'll need to address.

Gmail's Postmaster Tools

This **suite of tools** allows you to gather metrics on emails sent to Gmail users. Once you're set up in Postmaster Tools, here's what to keep an eye on:

- Domain and IP reputation are indicators of a healthy sender whose mail is hitting the inbox - both should be at a Medium or High. A dip to Low or Bad almost always results in mail being delivered to the junk folder, which you'll see paralleled by a dip in open rates at Gmail.

- Spam complaint rates should remain under 0.3% on a rolling basis - the lower the better.

We've put together this helpful checklist to make monitoring your deliverability easier:

List Management

- ❏ Filter based on recipient engagement activity.
- ❏ Put suppressions in place to send more frequently to active subscribers and less frequently to those less engaged.
- ❏ Use a re-engagement series or campaign for those subscribers who may not be active. Over time you should phase out sending to these subscribers if they don't engage after a certain period of time.
- ❏ Use a preference center so that you can capture your audience's preferences and give them an opportunity to opt-down or customize how and when they're contacted.
- ❏ Always track acquisition source and audit trail of permission.
- ❏ Use reCAPTCHA on sign up pages to prevent bots.
- ❏ Ask subscribers to add you to their safe senders list or address book. Review hard bounces, keeping your overall bounce rate under 1%. This is especially important for welcome series, as these messages are the first touch and will likely have the highest hard bounce rates.
- ❏ Generate and review regular reports that provide insight into bounces, complaints, and unsubscribes.

Technical

- ❏ Set up feedback loops with ISPs to record any users that mark mail as spam, allowing them to be removed from your list.
- ❏ Ensure authentication of each sender using SPF, DKIM, and DMARC on your sending domain.
- ❏ Ensure your ESP throttles email sends based on ISP SMTP (Simple Mail Transfer Protocol) response codes and optimizes mail to send at the correct speeds and rates.

Reputation Management

- ❏ Always gain explicit recipient permission and make sure you adhere to what they signed up to receive.
- ❏ Proactively monitor all email sends, addressing deliverability issues as soon as possible.
- ❏ Have real-time ISP block alerts in place.
- ❏ Monitor critical and impactful blocklists 24/7.
- ❏ Monitor drops in delivery rates and open rates.
- ❏ Monitor Spam Complaint Rates.
- ❏ Ensure you're following the ISPs' acceptable usage policies, as well as any legal regulations.

Where *relationships* take root.

Marigold's approach to relationship marketing stands alone in a world of one-size-fits-all marketing technology companies. Our solutions are designed for your specific size, industry, and maturity, giving you the technology and expertise you need to grow the relationships that grow your business, from customer acquisition to engagement to loyalty. And, with a team of strategists that provide insights into what's working, what's not, and what's changing in your industry, you're able to maximize ROI every step of the way.

MARIGOLD™