



eDATASOURCE

DELIVERABILITY



BEST PRACTICES GUIDE

A PRACTICAL GUIDE
TO PROTECT YOUR
INBOX REPUTATION
AND SUPPORT YOUR
ONGOING EMAIL
DELIVERABILITY GOALS



For professionals in email marketing, achieving great deliverability begins with a solid understanding of email best practices. And with today's constantly changing environment, it's nearly impossible to keep up with current trends. At the foundation of this understanding are practices that align with legal and regulatory compliance requirements that protect consumer rights. The lens we must look through is always the customer's.

Federal and Global laws are only a small part of safely managing inbox reputation, however, and all email marketing professionals must understand the importance of complying with a set of best practices meant to protect reputation and ensure strong, unrestricted email deliverability.

In this whitepaper, eDataSource provides readers with an extensive introduction to these best practices. Once you've put these best practices into place, monitoring and measuring your deliverability will be crucial. An easy way to start is to visit deliveryindex.org, enter your mailing domain, and see a quick snapshot of your deliverability over the most recent 30 days. You'll be able to check your inbox placement across all of the major ISPs, as well as key areas impacting your inbox reputation (including blacklists, spam trap hits, and authentication elements). You can also check your competition's sending domains to see how you measure up. It's free to use, and a great way to understand your deliverability and identify possible ways to improve it.

In the future, we'll be releasing more in-depth coverage of sending best practices, so don't forget to [sign up for our email newsletter](#) to get the latest and greatest from our resident industry experts.

TABLE OF CONTENTS

EMAIL MARKETING LAWS AND REGULATIONS

THE CAN-SPAM ACT 5
Best Practices Go Far Beyond Legal Compliance
The Basics
When Does CAN-SPAM Apply?

CANADA’S ANTI-SPAM LEGISLATION (CASL) 7
What Is Considered A CEM
Implied vs. Expressed Consent
Content and Record-Keeping
Unsubscribes

GENERAL DATA PROTECTION REGULATION (GDPR) 8
Consent
Opt-Out Duration
Penalties
Age Restrictions

ESSENTIAL BEST PRACTICES

EMAIL SUBSCRIBER ACQUISITION 10
Opt-In Best Practice
Subscriber Acquisition Methods and Sources

LIST MANAGEMENT 11
List Hygiene
Spam Traps
Pristine Traps
Recycled Traps

EMAIL CONTENT AND STRATEGY 12
Engagement Screening
Relevance
Frequency Optimization
Mobile Optimization
Subject Lines and Content Filters
Delivery Tracking

UNSUBSCRIBES, COMPLAINTS, AND FEEDBACK LOOPS 14
Unsubscribe/Opt-Out Process
Email Address Changes
Complaint Tracking
Feedback Loops
Outlook Postmaster Tools
Google Postmaster Tools

ESP AND IP REPUTATION 16
IP Address Warming
Shared IP Addresses
Multiple IP Addresses

AUTHENTICATION AND BRAND PROTECTION PRACTICES 17
Sender Policy Framework (SPF)
Domain Keys (DKIM)
Domain-Based Message Authentication, Reporting and Conformance (DMARC)

CONCLUSION

FOUNDATIONAL BEST PRACTICES 19

SENDER REPUTATION 20

APPENDIX 21



email marketing laws and regulations ▶

THE INS
AND OUTS
OF SENDING
EMAILS...
LEGALLY.

THE CAN-SPAM ACT

Introductory Note: *This document is not intended as a source of legal advice, therefore CAN-SPAM is not explained here in detail.*

In reference to this law, please remember that federal laws concerning email marketing were only created to limit abusive behaviors. Our professional perspective, and the widely accepted standard, is that compliance with federal laws does not even begin to cover the full extent of best practices that should be followed by email senders.

Best Practices Go Far Beyond Legal Compliance

While CAN-SPAM compliance will enable email senders to legally send emails, this alone does not prevent a sender from being considered a spammer by consumers, the ISP industry, or the email industry. The reality is that the CAN-SPAM Act has been referred to by some within the industry as the “You-Can-Spam Act” because of specific weaknesses associated with the bill including:

- Failure to prohibit email practices widely associated with spammers.
- Preempting specific state laws that would otherwise have provided spam victims with practical means of redress.
- Not requiring email senders to obtain permission before sending marketing messages over email.
- Preventing states from enacting stronger anti-spam protection.
- Prohibiting spam victims from suing spammers except under laws not specific to email.

The CAN-SPAM Act is critical in understanding email deliverability compliance. According to the Federal Trade Commission (FTC), the CAN-SPAM Act applies to all commercial messages, not only bulk emails. In the law, emails subject to the CAN-SPAM Act include:

“Any electronic mail message where the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.”

This includes any emails that promote content on commercial websites and no exceptions are made for business-to-business email. Under the CAN-SPAM Act, all email must comply with the law, even such examples as a message to former customers announcing a new product line.

Non-compliance to the CAN-SPAM Act is costly, with each separate email in violation subject to penalties of up to \$16,000. However, following the law isn’t complicated.

The Basics

Let’s take a look at the main requirements for remaining in compliance with the CAN-SPAM Act:

- **DON’T** use false or misleading header information. Accurate identification of the person or business initiating the email message isn’t optional. This means that your “From,” “To,” “Reply-to,” and routing information cannot include false or misleading information.
- **DON’T** use deceptive subject lines. Instead, ensure that all subject lines accurately reflect the content of the message. When in doubt, be direct not deceptive.
- **DO** identify the message as an ad. All commercial messages must clearly and intentionally disclose that the email is an advertisement. The law provides a number of ways to accomplish this.
- **DO** tell recipients where you’re located. Whether you have a street address, a post office box registered with the U.S. Postal Service, or a private mailbox registered with a commercial mail receiving agency, you must include a valid physical postal address in all emails. This also establishes credibility with your readers.
- **DO** tell recipients how to opt out of receiving future email from you. All emails must include a clear and conspicuous explanation of how the recipient can opt out of receiving future emails.



- Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand.
 - Creative use of type size, color, and location can improve clarity.
 - Give a return email address or another easy, Internet-based way to allow people to communicate their choice to you.
 - You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you.
 - Make sure your spam filter doesn't block these opt-out requests.
- **DO honor opt-out requests promptly.** You must honor a recipient's opt-out request within 10 business days. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message.
 - You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request.
 - Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.
 - In short, don't be tricky. If they want off your list, make it easy for them to do so.
 - **DO monitor what others are doing on your behalf.** It is ultimately your responsibility to comply with the law. The CAN-SPAM Act is clear that, even in the case the email management is contracted out, both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.

When Does CAN-SPAM Apply?

Here's how you can tell.

The primary purpose of the messaging being sent is the ultimate determination of whether or not the law is applicable to any given email. To provide further clarity, the FTC has defined three types of information that is sent in emails:



- **Commercial Content** advertises or promotes a commercial product or service, including content on a website operated for a commercial purpose
- **Transactional or Relationship Content** facilitates an already agreed-upon transaction or updates a customer about an ongoing transaction
- **Other Content** is neither commercial nor transactional or relationship

Compliance with the CAN-SPAM Act is required if an email's primary purpose is commercial and if it contains primarily commercial content.

In the case that an email contains primarily transactional or relationship content, it may not contain false or misleading routing information, but is otherwise exempt from most provisions of the CAN-SPAM Act.

Looking for more information about CAN-SPAM requirements?

Visit the Federal Trade Commission's website [page on the topic](#).

CANADA'S ANTI-SPAM LEGISLATION (CASL)

So how about emails from Canada or to Canada, eeh? We knew you'd ask.

Enacted in July 2014, Canada's Anti-Spam Legislation (CASL) differs from the U.S. version (CAN-SPAM), by penalizing noncompliance ranging from \$1 to \$10 million per violation. Email senders in Canada as well as sending emails to Canada are required to comply with CASL.

Unlike CAN-SPAM, CASL goes beyond the traditional scope of email and applies to any "Commercial Electronic Message" (CEM), including Short Message Service (SMS), sent from or destined to a Canadian computer or device in Canada. Messages from another country routed through computers in Canada are not subject to this legislation.

What Is Considered A CEM

Fair question, here's the scoop:

- Any message that is in an electronic format. For example, emails, instant messages, text messages, and even some social media communications, such as Twitter and Facebook.
- Any message that is sent to an electronic address, including email addresses, instant messenger accounts, phone numbers, and social media.
- There are many exceptions to the above, including messages sent to family members, employees and consultants. Most importantly, messages to current customers or someone who has inquired about a business relationship within the past six months are not required to comply with CASL.

Implied vs. Expressed Consent

CASL legislation requires email senders to have implied or expressed consent before sending CEM. If a recipient does not meet the implied consent requirement, then you must obtain expressed consent. Implied consent requirements include:

- The recipient has purchased a product or made any sort of transactional deal with a member of your organization within the past 24 months;
- You are a registered non-profit organization and the recipient has made a donation to your organization or attended a meeting organized by you or your organization;
- Your message is professional in nature and sent to someone whose address was given to you and the recipient has not published or stated they do not want unsolicited messages;
- If none of the above are true, then you must obtain expressed, written consent before sending CEM.

Content and Record-Keeping

CASL also stipulates that all emails must contain the sender's name, physical mailing address, phone number, and email or website address. Under CASL, records of expressed consent confirmations must be kept. When obtaining expressed consent, the default value must be unchecked and must not be prefilled.

Unsubscribes

Any message sent must contain an unsubscribe link and unsubscribe requests must be processed within 10 business days.

[Want to learn more about Canada's Anti-Spam Legislation?](#)
[Visit the Canadian government's website page on this topic.](#)

GENERAL DATA PROTECTION REGULATION (GDPR)

If the U.S. and Canada legalities weren't enough, we also have European Union compliance to consider. This is serious business, people, so please pay attention. Failure to comply can result in extreme financial harm to your business.

The General Data Protection Regulation 2016/679 (GDPR) is a regulation in European Union law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

If you send commercial email messages and are located in the EU or EEA or send commercial emails to the EU or EEA, there are four key requirements you must understand in order to remain in compliance with this law.

And we strongly encourage everyone to be aware of the requirements and to consult qualified legal counsel for compliance advice.

1) Consent

Senders must provide recipients with requests for consent that are separate from commercial email messaging. Within this messaging, the organization and any third parties relying on the recipient's consent must be clearly and accurately identified.

Similarly to CASL, pre-checked boxes do not count as obtaining consent. Each organization must keep records detailing the request for consent, including:

- What information was shared in the request for consent.
- When consent was obtained.
- How the recipient consented.

In short, they need to say "Yes, please email me," in some form or fashion before you email them.

2) Opt-Out Duration

Recipients can opt out at any time and requests must be honored promptly. Recipients also have the Right to be Forgotten (Data Erasure), which entitles the person or organization processing or disseminating any Personal Identifiable Information (PII) to halt the processing of that data. Conditions for erasure include the data no longer being relevant to the original purposes for processing or the recipient withdrawing consent.

If they say they want out, let them out. Pronto.

3) Penalties

Each violation will be fined up to 20 million Euros or up to 4% of the organization's total annual worldwide revenue, whichever is higher.

We imagine your boss won't like getting a penalty for "whichever is higher."

4) Age Restrictions

Before sending commercial email messages, the sender must obtain parental consent for children under 16 years of age. Member states can lower this age to 13 under GDPR.

Don't market to minors, that's not cool.

[Get further details on the General Data Protection Regulation on the European Commission's website page on the topic.](#)



subscriber acquisition methods/sources ▶

THE DO'S, DON'TS
AND OTHER TIPS
WE'VE LEARNED
ALONG THE WAY
AFTER ADVISING
OUR CLIENTS
ON BILLIONS
OF EMAILS



OK, now that we have the legal compliance covered, we can move on to the juicy stuff.

Although compliance with the legal regulations specific to CAN-SPAM, CASL, and GDPR is important, these requirements do not provide sufficient guidelines for avoiding spamming and abusive behaviors as a sender of commercial emails.

For this reason, we have included in this document an outline of best practices we believe are essential to respectful and reputable operation in the email marketing industry.

EMAIL SUBSCRIBER ACQUISITION

Everyone in the email world knows that email subscribers are the lifeblood of most businesses. So how should marketers get those valuable email addresses?

These best practices are concerned with establishing appropriate audiences for sending marketing emails or emails with commercial content. These opt-in requirements do not apply to transactional emails in which there is a clear business relationship transpiring.

Opt-In Best Practice

- **DO** use an active, positive opt-in protocol in acquiring email subscribers for your commercial or marketing emails. The consumer is clearly solicited for opt-in, and clearly knows they are doing so. This means they check a box which in essence says, *"Yes, I would like to receive (your) email. I think your company is super cool."* Well, at least that first sentence.
- **DO** follow-up the active opt-in with an email to the new subscriber, requesting that they confirm their opt-in. Or in other words, an email along these lines, *"Hey there, before we become email friends, can you confirm it was really **you** who signed up?"* Added bonus: you're keeping a clean list by ensuring your signups are from real people and not spambots!
- **DON'T** rely on any form of passive opt-in. The potential subscriber should never be automatically opted-in through some small print as part of a purchase transaction, with or without an option to uncheck an opt-in box, or to otherwise unsubscribe. If you have to hide the info to capture their email, do they really want emails from you?
- **DO** promptly acknowledge the opt-in, ideally with a welcome email to the new subscriber. A welcome email should arrive within minutes of the opt-in because, if the consumer forgets they subscribed to your email, they may view your subsequent emails as spam. And no one wants that.



Subscriber Acquisition Methods and Sources

So how do you grow a list, tactfully? And not all spammy-like? In general, the most productive source of new email subscribers are people already interacting with you as potential or actual customers.

Some examples include:

- Asking customers to sign-up for your emails during any purchase transaction. Transactional messaging such as purchase and shipping confirmations should also contain email opt-in calls to action. They clearly like you if they're buying from you, so ask away!
- Your website should have clear email sign-up calls to action. Pop-overs/lightboxes/modals which appear as the home page is initially loading are usually the most direct and persuasive way to collect emails. Adding email sign-up to your universal header and/or footer is also recommended.
- Your social media presence is an important source of email opt-ins. Leverage social media platforms by using clear calls to action to encourage your friends and followers to subscribe to your email list. You're "friends" now after all.
- Boost email subscriber acquisition by using a service which adds email addresses to your existing customer records who don't already have this information on file. eAppend vendors can identify email addresses that match your customer records and send a permission message to those customers to ensure deliverability and opt-in.

Note: We actively discourage the use of any other purchased email lists. In our experience purchased email lists tend to be expensive, unproductive, and a big source of spam complaints. Just. Say. No.

LIST MANAGEMENT

But how do you keep your email list vibrant, active and engaged?

Regular and thorough management of your existing list of email subscribers is a best practice that ensures only those who want to receive your emails are receiving them. This is a best practice that will protect the reputation of your organization by avoiding your emails being marked as spam.

List Hygiene

Good list hygiene results from continual maintenance. The more active and interested the email subscribers that make up your list are, the better. Address cleansing and a periodic change of email processing can help accomplish that.

- **Address Cleansing** is the act of subjecting all new email addresses to a basic screening, making sure they contain essential and valid elements. Your email service provider will almost certainly be performing this service. Because let's be real, HighSchoolGloryDays1973@aol.com is probably not checking email very often.
- **Periodic Email Change of Address (ECOA)** Processing is a practice adopted to account for the significant percentage of email addresses that become undeliverable every year. When emails 'bounce' or become longtime open/click inactives, this is a good indication that an email address is undeliverable. ECOA vendors can assist in finding the updated email addresses. Then, their service will send out a Permission Message to ensure both email deliverability and obtain permission to send the subscriber commercial messages at their new address. This message includes an email change of address link, permitting the capture of the customers' current preferred email address. Sounds complicated, huh? That's why a specialized vendor should do it for you using their own mailing infrastructure.
- **Facilitate Subscriber Email Change of Address** by including clear directions for subscribers to change their email address on your website. Did you know that a large number of email opt-outs are actually subscribers trying to change their email address? During the opt-out process (which we go into in greater depth later in this document), that protocol should include asking the subscriber if they're actually trying to change the email address, and if so, diverting to that process instead. Obviously, we'd way rather get their new email than have them unsubscribe from the list.

Spam Traps

In general, traps hurt those who get caught in them. A good life rule is to avoid traps of any kind at all costs.

A spam trap is an email address maintained by an ISP or third party, in order to detect poor practices in list management, list building, and deployment behaviors. Emails sent to these addresses never get clicked on or opened. If an address on your file has any recent activity associated with it, it is not a spam trap.

Spam traps are used by ISPs and third parties, such as consumer advocates and black list operators, to prove poor practices once a marketer hits one of those addresses. **Severity of response to hitting a spam trap differs based on the operator. In a worst-case scenario, one strike can be detrimental to general delivery either at the specific ISP, or — as is the case with blacklist operators such as SpamCop and Spamhaus — your email could be blocked universally, especially when multiple hits are detected.**

We were tempted to insert a crying face emoji here, but we'll just say it makes all email sending professionals sad to be blocked universally. OUCH.



There are two types of spam traps, Pristine and Recycled Traps

Pristine Traps

Pristine traps are email addresses that have never been used by an individual, but are decoys spread across the Internet on various sites, blogs, and forums. The intent is to lure spammers and list sellers who are illegally “scraping” addresses off the Internet to add them to their lists and expose their illegal or unethical behaviors.

Marketers who deal with list rentals or buy lists from less than reputable companies are often unaware of the negative legal and ethical ramifications and sometimes end up being the ones sending to these honeypot addresses.

There are only two ways a legitimate marketer should ever hit a pristine spam trap:

- Due to a mistyped email address from an individual subscribing to your list
- If an individual has left a fake address in order to avoid receiving emails from you.

To avoid pristine traps, it is always important to monitor new addresses on your list for activity and remove those that show no activity. Additionally, adopting a double/confirmed opt-in process eliminates almost all pristine spam trap hits.

And to think, they'll miss the content gold of the confirmation email announcing we're email BFF's.

Recycled Traps

Recycled traps are email addresses that once belonged to a user, but have been abandoned or closed for a long period of time. These sometimes get reactivated and recycled in order for the operator to see who does not clean their lists and remove inactive addresses, indicating poor list management practices. These are often operated by ISPs in order to filter and deprioritize email from these companies that send to these addresses, ultimately causing moderate to severe inbox issues for the sender.

Use of confirmed opt-ins, good list hygiene, and regular pruning of inactive subscribers is the most effective way to avoid spam traps altogether.

Kind of like those pesky hedges in the front yard, a good pruning goes a long way to boost curb appeal.

EMAIL CONTENT AND STRATEGY

Keep email subscribers engaged with relevant email content and avoid emailing consumers who simply aren't engaged with your message. To put it directly, you gotta give 'em the good stuff to keep them happy.

Engagement Screening

Avoid emailing any customer who has not opened or clicked your email, browsed your website in the past 90 to 120 days, or bought in the last twelve months.

They're trying to tell you something, they're just not that into you.

Before you can establish accurate customer activity status, you need to be able to see your customers' multi-channel purchase and summarized browse behavior in a 360-degree customer-level database.

Who owns your CRM database of record? Using that database in managing your email programs and defining customer status is an email marketing best practice you can't afford to miss.



Mitigate risk by considering initiating a re-opt-in or reactivation program for inactive email subscribers. These programs acknowledge unengaged subscribers and give them the choice to re-opt-in to continue receiving your email messages.

Basically, we're asking, "So, you're saying there's a chance?"

Relevance

A large driver of spam complaints and email opt-outs are customers receiving email in which they see nothing of interest. Mass mailing ("batch and blast") email is a considerable source of this issue. Email is much more likely to be considered acceptable and engaged with if the subscriber sees it as relevant.

Relevant email meets the following standards:

- **Lifecycle Management:** Messages are part of an integrated program addressing subscriber lifecycle waypoints. These waypoints include acquisition, welcome, activation, cross-sell, up-sell, retention, and reactivation.
- **Segmentation:** Messages are targeted to specific audiences based on subscriber profile, preferences, location, and their browsing or purchase behaviors.
- **Personalization:** Messages contain customer first and/or last name. Content may be keyed to customer age, gender, status, preferences, behavior, or social network participation.
- **Triggers:** Behaviors or events triggers email messages where possible.
- **Interactivity:** Email facilitates customer engagement and response through links to purchase activity, communication, entertainment, preference centers, and surveys. Messages can be socially shared and encourage the subscriber to join the brand's social networks.

Frequency Optimization

Over-mailing is another source of email spam complaints and opt-outs. Determining how much is "too much" is a matter for testing different frequency cadences across various customer engagement segments.

In the absence of test data, we believe that subscribers receiving more than four promotional or marketing email messages per week from a single mailer may be at risk for reporting these emails as spam. It's easy to set and forget your automated messaging streams. Take the time to review these and verify the targeting and cadence is operating the way that the program was designed.

You don't want to get to that spot where the reader is saying, "Oh great, you again..."

Mobile Optimization

Email opens on mobile devices, including tablets, now account for over 60% of marketing email opens, and that mobile-engagement share continues to rise. All emails sent should be optimized for proper rendering on mobile devices. Email that is not mobile-optimized has a much greater likelihood of being deleted, unsubscribed, or moved to the spam folder.

And also a great likelihood for an eye roll.

Subject Lines and Content Filters

Spam filters use a long and unpublished list of criteria when judging how "spammy" an email is. Many factors go into the building up of a spam score, which ultimately then determines whether an email will be delivered to the inbox, the spam folder, or outright blocked at the sender-level before ever arriving in your subscriber's mailbox. Two of the most critical pieces in the generation of this spam score are your subject line and the content of your email.

- Avoid use of subject lines that look spammy, as your email will undoubtedly be recognized as such by the spam filter. Phrases such as, "BUY NOW!!!", "FREE OFFER!!" and similar phrases will be assigned points each time they are found. If you get enough points, your mail is delivered to the spam folder. Not the folder where you want your email to land.
- Be aware of how phrases can be grouped into different high-level categories. These categories are then assigned points by email filtering programs. If any message gets assigned too many points (the default is usually 5.0), it gets sent to the spam folder.

The open-source SpamAssassin provides some insights into these categories and how they are assigned:

- Mortgage email? .297 points
- Contains words that imply urgency or importance? .288 points
- Money back guarantee? A whammy at more than 2 points

- While there's no guaranteed way to avoid spam filters, there are some common practices and mistakes that can improve your chances of landing in the inbox.
 - Avoid phrases which overtly try to entice a user action, such as "Click Here!"
 - Avoid using multiple special characters in your subject lines. More than one exclamation point will, in almost all cases, be immediately flagged as spam. Even valid phrases such as "*We released a new feature! Come check it out!*" will significantly increase your spam score. A better subject such as: "We released a new feature. Come check it out!" will be scored much lower. And people won't think you're soooo excited all the time!!
 - Everybody hates screaming, including spam filters. Do not use ALL CAPS. UNDERSTAND?
 - Avoid sending an email with only a single image. Most spam filters can't determine what an image represents and will mark a message that is just an image as spam, regardless of how non-spammy it is.
 - Make sure your HTML is valid. Spammers are notorious for having poor HTML. Modern spam filters look at the validity of your HTML as much as the content. Coders unite.
 - Avoid links that look like phishing links. If your link goes to a significantly different URL than your text does, many modern filters will consider this a phishing attempt and mark the message as spam. Avoid using URLs in the content of your text, and instead use words. Example: `sign up` instead of `www.mycompany.com/signup`
 - Ensure your background and text colors are not too similar. Spammers will often hide text by making the background and text colors the same. This tactic is usually caught by spam filters. And even if it doesn't, it looks terrible.

Delivery Tracking

You and your ESP should be tracking the deliverability of your emails on a daily basis, by ISP. Issues need to be identified and acted-upon quickly.

UNSUBSCRIBES, COMPLAINTS, AND FEEDBACK LOOPS

In compliance with the anti-spam laws mentioned above, adopt best practices concerning unsubscribes, complaints, and feedback loops.

Unsubscribe/Opt-Out Process

Even though the basic principles of unsubscribe best practices are covered in the CAN-SPAM section earlier in this document we've added some additional details below.

Opt-Out Should Be Clear

Your message must include a clear and conspicuous explanation of how the recipient can opt-out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand.

- Creative use of type size, color, and location can improve clarity.
- Give a return email address or another easy Internet-based way to allow people to communicate their choice to you.
- You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you.
- Make sure your spam filter doesn't block these opt-out requests.

The Opt-Out Process Should Be Easy

- Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request within 10 business days.
- You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an internet website as a condition for honoring an opt-out request.
- Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.

Enable The List-Unsubscribe X-Header

List-Unsubscribe is a special X-Header that is added to the headers of your outbound email by your ESP. It enables ISPs like Gmail and Outlook.com to offer a one-click method of unsubscribing from unwanted emails instead of reporting it as spam.

For more information about List-Unsubscribe visit [List Unsubscribe on the web](#) and read [this brief on the topic](#).

Email Address Changes

As mentioned above, many opt-outs are subscribers who simply want to change their email addresses. To retain engaged subscribers, your opt-out protocol should include the following, “If you’re trying to change your email address, please click here,” diverting subscribers to a change-of-address landing page. This is an opportunity to save a considerable number of email addresses and their associated history.

That’s a recovery effort worth pursuing.

Complaint Tracking

Complaints come in the form of direct complaints and “report spam” complaints. All complaints should be tracked and patterns in complaints should be used to make adjustment to email practices.

“**Report Spam**” Complaints occur when a recipient clicks the “Report Spam” button within their email program or webmail interface. This type of spam complaint can have a fairly significant impact on your deliverability reputation. If enough users mark your messages as spam, then your reputation at that ISP will drop and you may see your other messages going to the bulk folder.

Feedback Loops

Many ISPs provide a Feedback Loop (FBL) Notification system that supplies marketers with insight into the subscribers who are clicking the “report spam” button. Marketers are able to register an email with the ISP for receiving FBL reports. Each time a recipient clicks the “report spam button,” the system generates an abuse report and sends it to the provided email address. This is one of the most useful resources available to marketers in regards to gaining insight into what email behaviors are being seen by subscribers as spammy.

Abuse reports also provide marketers with the information they need to take proactive action, stopping emails to recipients who report their messages as spam or at least being more selective about the types of emails sent to those recipients.

Outlook Postmaster Tools

Microsoft offers two different postmaster tools to help with your reputation monitoring. The **Microsoft Junk Mail Reporting Program** (JMRP) and **Microsoft Smart Network Data Services** (SNDS).

Microsoft SNDS is a fantastic resource that marketers can use to responsibly monitor their IP email deliverability and reputation at most Hotmail and Outlook email addresses. Microsoft SNDS covers outlook.com, hotmail.com, msn.com and live.com email addresses. (note: Office365 is not covered by SNDS)

Microsoft SNDS is an invaluable tool all email marketers should be utilizing, providing you with insights into various metrics, including:

- Total number of messages which were attempted to be delivered
- Total number of recipients who actually received the message
- A look into how the Microsoft spam filters handled the messages
- Complaint rates
- Examples of headers and messages that caused high complaint rates

Learn more about Microsoft SNDS on their [Frequently Asked Questions](#) page.

Google Postmaster Tools

Most email marketers' lists are heavy with Gmail accounts. Gmail is very transparent about what it expects from email senders, providing a Bulk Sender's Guide for reference.

Gmail also provides a set of Postmaster tools that can be used to monitor deliveries made to Gmail accounts.

These tools will indicate:

- If users are marking your emails as spam.
- Whether you're following Gmail's best practices.
- Why your emails might not be delivered.
- If your emails are being sent securely.

Learn more about Google Postmaster tools from [Gmail Help](#).

ESP AND IP REPUTATION

Sender and IP reputations are likely the most important factor in determining if a sender's emails are marked as spam or delivered to the inbox. Similar to the content scoring mentioned above, ISPs assign a score to a sending IP address and domain based on current and past sending patterns and behaviors.

It's not much different from real life. Your reputation matters. How you operate is important.

Unfortunately, scoring is complicated, since each ISP determines scoring in a slightly different manner. In light of this, we have provided some of the common best-practices to ensure a strong reputation among all ISPs.



IP Address Warming

When sending email from a new IP address, the ISPs have no information that allows them to make a determination of how reputable a sender you will be over time. Because of this, it may be necessary to warm an IP address before sending commercial emails.

Typically, for senders delivering a low volume of email each month (<10,000), IP warming is not critical. However, if a sender delivers more mail than this threshold, IP warming is a strongly suggested practice.

Since the process of warming an IP address is beyond the scope of this document, you will want to consult your ESP. They can walk you through their specific process and any recommendations they have for IP address warming.

Shared IP Addresses

There are pros and cons to this practice, so it's important you understand your own sending patterns to determine whether a shared or dedicated IP address is more appropriate for your business.

• Pros of a Shared IP

- One of the strongest benefits of a shared IP address is that the volume has already been established for a consistent and long period of time. This makes it easier to get your mail delivered into the ISPs inboxes.
- The ability to share reputation can be beneficial for low-volume senders who have sporadic or inconsistent email sending patterns. The ability to "piggy-back" on the IP reputation of other reputable senders can bolster your own.
- Shared IPs traditionally cost less than dedicated IPs.

• Cons of a Shared IP

- When using a shared IP address, you have zero control over the send patterns or content of the other senders on the IP. Despite this loss of control, their content and send patterns directly impact your IP reputation.
- Yes, we're repeating ourselves — shared reputation is also a downside of a shared IP address. Your reputation is shared amongst all your neighbors, and if your neighbor's IP reputation goes south, yours probably will too. Remember, you are the company you keep.

Multiple IP Addresses

In the past, one way that senders got around spam filters was by sending their email across multiple IP addresses. This tactic is known as “snowshoeing.” For the most part, it no longer works and can significantly harm your IP and domain reputation.

For very large senders, there are some cases where sending across a handful of IP addresses may benefit the reputation and increase deliverability. For the vast majority of senders, using one or two IP addresses is the appropriate choice.

Ultimately, you will want to consult with your ESP on their specific recommendations for your send profile.

AUTHENTICATION AND BRAND PROTECTION PRACTICES

Email authentication, or confirming the real identity of the email sender, is one of the top factors in your email reputation. Authentication allows the ISP to confirm that your email really came from you and is not the work of a spammer or a phishing attack.

The landscape for email authentication involves three distinct frameworks: Sender Policy Framework, Domain Keys, and Domain-Based Message Authentication Reporting and Conformance.

Each of these frameworks has a slightly different purpose. Every major ISP values and treats these frameworks differently, so it is strongly suggested that you always include all three in your email sends.

Sender Policy Framework (SPF)

SPF allows senders to specify which hosts are allowed to send email on behalf of their sending domain. Administrators generate a specific SPF record in their public DNS. Mail Exchanges then use this DNS record to verify that the message was sent by a trusted party.

Domain Keys (DKIM)

DKIM (pronounced DEE-Kim) allows organizations to accomplish two things. First, DKIM guarantees the sender is who they say they are. Secondly, DKIM guarantees the contents of the message.

DKIM utilizes public-private key cryptography to provide these guarantees. The sender signs the message with a signature that only they know, and the encrypted signature is then attached to the message and sent to the recipient. When the message arrives at the destination, the server asks the sender for the public key which can then be used to verify the message is authentic and was actually sent by the sender.

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

DMARC is the latest standard created to prevent phishing attacks. In many ways DMARC is built on top of both SPF and DKIM and standardizes the two.


Using DMARC allows a sender to build a policy communicating, “All valid email sent from a server I trust will be authenticated in this particular way. Any invalid email will be discarded, and I will be notified that someone is trying to send as me.”

There are three basic parts of DMARC.

- 1) DMARC provides a way to confirm the “from domain” is authentic using both the DKIM and SPF authentication results. DMARC builds on top of this by allowing the sender to define how the “from domain” has to “align” — strict or relaxed. If the alignment is **strict**, then the domain match must be exact. For example, if the from address is hello@email.com but the actual sender was hello@sender.email.com this would be considered an unaligned email message. Similarly, if the alignment is **relaxed**, then subdomain matches are allowed. In our example above, with a “relaxed” policy the message would be “aligned.”
- 2) DMARC provides a framework to tell receivers and spam filters what to do with messages that are not DMARC-aligned. If a sender can guarantee that all of the email it sends will be aligned, then through DMARC they can publish a policy telling the ISP to “always delete unaligned email” or “always put unaligned email in the spam folder.”
- 3) DMARC also provides a reporting feature. This allows organizations to find sources of legitimate, but non-DMARC aligned mail, so they can fix it and ensure it is aligned. Additionally, this reporting feature can help senders to track down and prevent phishing attacks.

The background features a light blue and white abstract design with several blue checkmarks in rounded square boxes, a bar chart with upward-pointing arrows, and a grid pattern. A vertical green line runs down the right side of the page.

conclusion ►

A close-up view of a blue grid pattern, possibly representing a screen or a data visualization, with a blue checkmark visible through the grid.

ACHIEVING PEAK
INBOX PLACEMENT
AND EMAIL
DELIVERABILITY
NIRVANA



FOUNDATIONAL BEST PRACTICES

According to eDataSource research, inbox deliverability on average in the B2C brand marketing world is about 81%.

If yours is better than that, you are doing a good job. Give yourself an 'attaboy' or 'attagirl'.

If you are below that, you should address some of your practices and be more constructive in the management of your program. The most important issues that may negatively affect your delivery are:

- 1) Addresses that are inaccurate and cannot be delivered
- 2) Delivery to addresses that are no longer valid and have been converted to "spam traps," giving your overall deliverability and history a negative strike
- 3) Complaints or "report spam" button hits
- 4) Ineffective removal of unsubscribed or undeliverable addresses
- 5) Black lists
- 6) High volume or frequent delivery to low or no activity addresses
- 7) Inconsistencies in list sizes and frequencies, meaning, for example, not sending emails for a couple of weeks, but then sending every day; or to periodically sending to your non active file, such as by suddenly including non-active subscribers in large deployments, before major promotional periods. This is a common temptation that many fall for before major holidays, and tends to end with a disaster. Or maybe with someone losing their job. Too dramatic? Yeah, probably, sorry about that.

Best practices are the reverse of the issues listed above.

- 1) Make sure that new addresses are verified and correct, most easily achieved by sending a confirmation email upon sign up.
- 2) Clean up and remove inactive subscribers, or those that have not opened an email in 3-6 months.
- 3) Immediately remove any unsubscribe and bounces.
- 4) Work up to higher frequencies, meaning that higher frequency should not be used to combat lower engagement. Instead, frequencies should be increased over time rather than suddenly.
- 5) Be human and treat every email you send like a real, live conversation.

In short, ISPs like senders that have predictable, well thought through email programs that their inbox users don't complain about.

Don't think for a minute that you will be able to outsmart ISPs in the long run by utilizing multiple IP addresses, snowshoeing, piggy-backing on shared IP pools, or constantly changing IP addresses or sub-domains.

These are all short-term, unethical approaches to fix deliverability. While they may sometimes work for a week or two, the only long-term solution is to follow best practices. All you need is a little bit of discipline and systems that help you carry out best practices.

SENDER REPUTATION

Following basic foundational best practices builds your reputation as a sender. You should keep a consistent sending domain and preferably a single IP address per class or segment of messaging. For example send your Welcome messages from one IP, your transactional messages from another and your marketing messages from another. The old practice of sending your best subscribers on a “safe IP” and your questionable addresses on a “high risk IP” is no longer sustainable. ISP’s are now monitoring both your IP level reputation and your domain level reputation and are scoring and controlling your inboxing based on these reputations.



THERE ARE NO SHORTCUTS

Beware of any companies that tell you that you can pay them to get your email delivered. Most of the companies that have promoted such an approach are now out of business. It has been verified countless times by both Email Service Providers as well as brands and research companies like eDataSource that paying for preferential treatment does not get you out of the spam folder.

In fact, it's just a waste of money.

Keep in mind that ISP's service their inbox subscribers. They are the bread and butter of their business. If you think they would risk that relationship with their inbox subscriber by allowing third parties to buy their way into their clients' inboxes...well we have some beach-front property in Kansas we'd like to sell you.

That would erode the trust that the general public has in their service and ultimately ruin their business.

CONGRATS, YOU MADE IT!

It was a long read but worth it in your quest to achieve email deliverability greatness. We're sure it feels overwhelming, and there is always more to learn, but that's why we're here. Our resident email experts are on standby, waiting to help take your email deliverability game to the next level. Give us a ring, or an email, and we'll come running.

HAPPY SENDING (AND DELIVERING TO PEAK INBOX PLACEMENT).

APPENDIX

HELPFUL LINKS

Looking for more information about CAN-SPAM requirements?

Visit the Federal Trade Commission's website page on the topic.

<https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>

Want to learn more about Canada's Anti-Spam Legislation?

Visit the Canadian government's website page on this topic.

<https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home>

Get further details on the General Data Protection Regulation on the European Commission's website page on the topic.

https://ec.europa.eu/info/law/law-topic/data-protection_en

For more information about List-Unsubscribe visit:

<https://www.list-unsubscribe.com>

Or read this brief on the topic:

<https://www.ietf.org/rfc/rfc2369.txt>

Learn more about Microsoft SNDS on their Frequently Asked Questions page.

<https://sendersupport.olc.protection.outlook.com/snds/FAQ.aspx>

Learn more about Google Postmaster tools from Gmail Help.

<https://support.google.com/mail/answer/6258950>