



White Paper: **Winning Email Marketing Campaigns**

Executive White Paper

While companies continue to invest in multi-channel marketing to deliver relevant messages across an array of media and channels, the email channel provides its own unique challenges to getting that message delivered. The following is a collection of technology solutions and best practices that promote the delicate balance between effective, compelling and compliant email creation and delivery.

Taking the Right Steps

The email marketing channel provides its own unique challenges to getting that message delivered. Only a combination of technology, the right lists, best practices, and constant vigilance will result in favorable delivery rates for email marketing messages. The days of simple, open email exchange are a thing of the past as email has become an increasingly complex medium, both through its widespread popularity and the variation that tends to go along with that kind of growth.

These days, email publishers and recipients alike are trying to strike a delicate balance. Publishers want their messages to be delivered reliably and to be read, while recipients want their email to arrive in manageable quantities and to be free from fluff, filler, and hype.

Many of the principles that follow here have withstood the industry's own test of time, proving over and over again that they work in favor of both the people who create email messages and the people who receive them. In addition to creating harmony between publisher and recipient, best practices help publishers accomplish their most important goals: keeping lists populated by active members, delivering mail without being inappropriately blocked by filters, and creating email content that's opened and acted upon. Because they promote habits that meet or exceed most legal requirements, email marketing best practices also help publishers stay on the right side of ISPs and the law.

Step 1: Choosing the Right Partner

The first step to delivering email marketing messages is to work with an Email Service Provider (ESP) – such as Healthcare Dialog's sister company Redi-Mail that has the right combination of technology and industry expertise to ensure your messages reach their intended audience.

ISP RELATIONSHIPS

While it's tempting to see ISPs and other email providers as an obstacle between you and your target audience, like you, they want to make sure that their subscribers receive legitimate opt-in email. ISPs that don't care about this and reject large quantities of legitimate mail would soon find themselves losing clients. But they also need to protect their subscribers from the current tidal wave of truly unsolicited, unwanted mail. As spammers get craftier, ISPs are forced to enforce stricter rules to filter out mail that looks like spam. Sometimes, despite best efforts, it might be your mail that gets filtered. Redi-Mail and Healthcare Dialog work with the major ISPs to comply with their processes and work with them in a constructive manner to ensure that messages are delivered, and opt-out requests are respected.

White Lists & Feedback Loops

ISPs such as AOL offer "white listing" of IP addresses for clients. In order to maintain a positive standing with these ISPs, it is important to comply with their feedback loop processes. When recipients receive marketing messages, these ISPs provide a mechanism to notify Redi-Data of an unsubscribe request that must be respected, and Healthcare Dialog will automatically unsubscribe that recipient. While this may help deliver more of your mail, remember that such a positive relationship with the ISPs does not mean that you can send unsolicited or unwanted mail without negative consequences.

Bounce Processing

A critical factor when sending to ISPs is how many of the messages are being sent to invalid email accounts. If ISPs notice a high bounce-rate coming from an IP address, they are far more likely to block that IP address or remove the IP address from their white lists. We automatically detect bounce backs and categorize them based on the severity of the bounce.

Hard bounces, such as bad mailboxes, are immediately flagged as such and removed from future mailings. Softer bounces – like full mailboxes and out of office replies – are monitored, and if too many soft bounces occur over time, the email address will be removed from future distributions as well.

DEDICATED IP ADDRESSES

Each client receives two or more dedicated IP addresses that are not shared with any other clients and it's from these addresses that the platform always delivers email messages for that client. If an ISP decides that too much bulk email is being delivered from an IP address, it may choose to temporarily or permanently block that IP address. Because each client receives its own dedicated IP addresses, one client cannot negatively impact other clients on that same server. The platform notifies Healthcare Dialog's deliverability team of the blockage and they can contact the ISP on behalf of a client to resolve the issue.

AUTOMATED IP SWITCHING & DOMAIN DELIVERY THROTTLING

When an ISP chooses to block a client IP address, our Message Delivery Servers will automatically throttle-down the delivery of messages from that client to that ISP. The servers will also switch the IP address to another IP address for that client, hopefully resolving the blockage. In some cases, the deliverability team will still need to contact the ISP to resolve blockages.

CUSTOMER - SPECIFIC URLS

In order to enable features like link tracking, open HTML reporting, bounce back handling and many others, ESPs often replace client's links and from addresses with their own so that they can implement a feature. For example, instead of sending an email from marketing@client.com the ESP often wants to track responses to the "from" address, and so it sends the message from client@esp.com. This can have several negative effects on the delivery and reputation of the marketer. Recipients notice that the email doesn't appear to be coming from the marketer's domain, but from some third-party unknown domain. Also, if another client of the ESP gets blocked by one or more ISPs, now all of that ESP's clients are blocked as a result. We work with clients to set up company - specific URLs (i.e., msg.client.com and links.client.com) for click - through tracking and from addresses. Those URLs point to our sister company - Redi-Mail's -servers so that all of the expected functionality works, without incurring the negative impacts.

DOMAIN AUTHENTICATION COMPLIANCE

ISPs like Hotmail, Yahoo, Google, and others utilize various domain authentication mechanisms to validate and verify that messages that are allowed to be sent on behalf of a company.

Reverse DNS

Because DNS is such an important way of establishing identity on the Internet, spammers will often forge domain names or IP addresses to hide the source of their mail. To detect these forgeries, ISPs perform a reverse DNS lookup on incoming messages. This type of lookup takes the IP address that's trying to make the connection and checks to see if there is a registered domain associated with it. If it doesn't match, the message may be a forgery - or, the hapless sender may have an incorrect DNS entry. In either case, the ISP will most likely treat the message as spam. All messages sent from client-dedicated IP addresses have the necessary reverse DNS look up records and will authenticate correctly. Special "PTR" domain records are set up to ensure that this look up functions correctly.

Sender ID / SPF

One form of authenticating incoming email is SPF, or Sender Permitted Framework. In a nutshell, SPF is just a single line within your DNS entry that identifies which IP addresses are approved to send email for your domain. We work with clients to ensure that their customer - specific URLs and DNS records have the necessary TXT record to comply with SenderID/SPF. An SPF record looks like this: msg.client.com IN TXT " v=spf1 a mx include:spfhost1.cv47.net - all"

DomainKeys / DKIM

Another form of authenticating incoming email is DomainKeys, which was created by Yahoo.

How it Works - Sending Servers

There are two steps to signing an email with DomainKeys:

- 1) **Set Up:** We generate a public/private key pair to use for signing all outgoing messages (multiple key pairs are allowed). The public key is published in the client's DNS records, and the private key is made available to our DomainKey-enabled Message Delivery Servers.
- 2) **Signing:** When each email is sent, we automatically use the stored private key to generate a digital signature of the message. This signature is then pre-pended as a header to the email, and the email is sent on to the target recipient's mail server.
- 3) **Delivering:** The receiving email system applies local policies based on the results of the signature test. If the domain is verified and other anti - spam tests don't catch it, the email can be delivered to the user's inbox. If the signature fails to verify, or there isn't one, the email can be dropped, flagged, or quarantined.

How it Works - Receiving Servers

There are three steps to verifying a signed email:

- 1) **Preparing:** The DomainKeys - enabled receiving email system (such as Yahoo) extracts the signature and claimed From: domain from the email headers and fetches the public key from the client's DNS records for the claimed From: domain.
- 2) **Verifying:** The public key from the client's DNS records is then used by the receiving mail system to verify that the signature was generated by the matching private key. This proves that the email was truly sent by, and with the permission of, the claimed sending From: domain and that its headers and content weren't altered during transfer.
- 3) **Delivering:** The receiving email system applies local policies based on the results of the signature test. If the domain is verified and other anti - spam tests don't catch it, the email can be delivered to the user's inbox. If the signature fails to verify, or there isn't one, the email can be dropped, flagged, or quarantined.

ANALYZE CONTENT & DELIVERY

We provide the necessary tools to analyze and audit the content and ISP delivery rates of email marketing messages.

Content Analyzer

Content that triggers spam filters is not always obvious. The Content Analyzer tests your message for spam filter triggers and advises you of possible problems before you send your campaign or transactional emails. It also checks for issues in the email header that you may not even realize are important. When you conduct an audit, the Content Analyzer tests your message against more than 30 different spam filters. Most of these filters that Content Analyzer checks use a scoring system to rate the relative "spamminess" of your message, and some indicate which elements of your message are most representative of unsolicited mail.

ISP Delivery Monitor

Delivery Monitor is a powerful tool for gaining valuable, real - time information about your campaigns - are they being delivered at all and, if so, are they making it to recipients' inboxes. Use Delivery Monitor to determine if your mail is automatically routed to "spam" or "bulk" folders at more than 50 different ISPs and email providers, and then take corrective steps to delivery more mail to the one place it will be read - the inbox. This process not only advises you if your mail was blocked, delivered to the inbox, or automatically routed to a "spam" folder, but also indicates if deliverability to a particular ISP changes during the course of a campaign. Delivery Monitor checks 20+ U.S. ISPs and 20+ European ISPs such as EarthLink, AOL, Yahoo!, Hotmail, and many more.

By running a Delivery Monitor audit, the software:

- Provides real - time feedback about email deliverability to more than 30 different ISPs and email providers.
- Reports deliverability issues based on what end users actually see in their mailboxes—not by POPping mail accounts, an easier but less accurate measuring method.
- Indicates if deliverability problems arise during a campaign, so you can pause the mailing until the issues are resolved.

Black List Monitor

Even marketers that mail with permission may be inadvertently and incorrectly blacklisted. The Blacklist Monitor tells you if any of the major blacklist organizations have targeted the domains referenced in your email campaigns so you can take appropriate steps to resolve the blockages and deliver mail as intended.

Inbox Snapshot

Inbox Snapshot generates several reports: one shows you how your email will render. It will also display the HTML, spell check it, and show you where your message may have issues so you can correct them before you send to your entire list. Inbox Snapshot audits your message in popular email clients such as Outlook, Hotmail, Yahoo!, AOL, Gmail, and more.

Step 2: Best Practices

Even with great technology and competent partners like Healthcare Dialog and Redi-Mail, it is still up to the marketer to follow industry best practices to ensure that their marketing messages are being delivered to the inbox. This section covers the essential email marketing best practices that will collectively increase your list size, improve your response rates, and help you stay on the right side of Internet Service Providers and the law. We've organized these eight best practices in a logical order—from initial list creation to results analysis—and suggest that novice email marketers read them straight through. If you're seasoned, of course, just select the topics that are most of interest to you.

BEST PRACTICE 1: MAIL WITH PERMISSION

Best Practices start with the manner in which you create and build your email list. The most effective approach is to use an "opt-in" or "permission-based" subscription process, such that individual people give you their explicit permission to contact them via email.

Use a "double opt - in" subscription process

The highest, most ethical subscription standard is called double opt - in, and it requires prospective subscribers to actively confirm their membership before receiving your next mailing. In this process, prospective subscribers submit their email addresses and then receive confirmation requests to which they must reply in order to join your list. Requiring prospective members to confirm their membership protects them from receiving mail they didn't sign up for - say, because someone made a typo when entering the email address or because someone thought it was funny to add a "friend" to your list. Best of all, those who confirm their subscription are most likely to remember it when they receive your email, making it less likely that they'll report the message as spam.

When you make your list double opt-in, tell your prospective members to expect the confirmation email and the address from which it will come. Explain why you do it this way and why this practice protects them. You might also suggest at this point that the recipient "white list" you by putting your "From" address in their address book to assure your mail is always received in their main mailbox. Also be sure that the marketing software or service that handles your email subscriptions delivers the confirmation request to prospective members promptly so that their decision to join your list is still top-of-mind.

Recipients who receive confirmation requests within a minute or two of subscribing will be far more likely to complete the confirmation process. The double opt - in subscription process offers many benefits:

Pros

- Builds an audience that truly wants to hear from you: these people have joined your list because they believe you're going to send them something of value.
- Increases mailing delivery rates because double opt-in lists are inherently comprised of valid, deliverable addresses (at least until some addresses are cancelled in the normal course of Internet life).
- Keeps your lists clean. Clean lists are delivered faster because the list server doesn't spend time retrying bad addresses. And if you use an Email Service Provider that charges based on your membership, clean lists mean lower hosting bills because you aren't sending messages to recipients who don't exist.
- Helps maintain good ISP relations. By maintaining a list comprised of legitimate addresses, most of your mail will be delivered successfully. If you send large quantities of mail to invalid addresses, ISPs or other email providers may blacklist you and block all of your mail.
- Increases response rates. Double opt - in not only confirms a recipient's email address but also confirms the recipient's interest in what you have to offer.

Cons

- Some prospective list members will not confirm their subscriptions. (You don't want these people anyway; if they can't be bothered to complete their subscription, how likely is it that they'll buy something from you?)
- Requires more patience to build a large list. If you have 10 thousand addresses and want to grow to one million, the double opt - in process will take some time. It can be very tempting to take a shortcut and rent or purchase a list of addresses, but those are not Best Practices.

Alternatively, use a “single” or “confirmed opt - in” process

Some email marketers and publishers choose a simpler subscription process. The single opt-in method consists of one basic step: a subscriber provides his email address to you through a Web form, email, or some other channel, and then receives your next mailing with no further administrative steps. If you add another step - sending the subscriber a one-time confirmation message (e.g., “Thank you for joining...”) - then you're using a confirmed opt-in approach. While these two approaches have good intentions, they still allow non - permission based subscriptions to occur. With good, humorous, or malicious intentions, a user may sign up her “friend” to your list; that person may then react negatively towards your organization if they don't expect (or if they object to) your mailing.

There are circumstances where single-opt in makes sense, such as for a trade organization that requires a login to access the subscription form. In this case, the opportunity for mistakes or abuse would be remote.

Include valid unsubscribe instructions in every message

Permission to send mail is not permanent. Over time, some number of people in your database will no longer want to hear from you, for any number of reasons. Enabling these members to remove themselves from your list quickly and easily will maintain the trust you previously established and perhaps leave positive feeling, making it more likely that some of them will re-subscribe at a later date. By including a one- or two- click unsubscribe function in the footer of each message, you'll show the public that you're an ethical marketer, differentiate yourself from truly unsolicited email and comply with the law (see Best Practice #7).

Don't use an “opt-out” subscription process.

Some Web sites include “opt-out” checkboxes or radio buttons on their e-commerce pages, such that shoppers are automatically subscribed to a mailing list upon checkout - unless they notice that part of the form and select the alternative. This subscription approach may lead to a larger initial number of addresses if you have an active shopping site, but may lead to complaints down the line. If your recipients don't remember asking to receive your email, they may consider the appearance of your messages in their inboxes as an intrusion and a breach of the trust they placed in you when they placed an order on your Web site. Sometimes, salespeople are tempted to dump their entire list of contacts and prospects into their mailing list, reasoning that anyone on the list

must still be interested in their services and can always opt out when they receive the messages. Just because someone has contacted you in the past does not mean they wish to continue that contact in the future!

BEST PRACTICE 2: SET AND MEET EXPECTATIONS

One of the easiest mistakes list owners make is to send content that their list members don't expect to receive. This happens most often when subscriber expectations aren't well managed from the start; if the sign-up form doesn't describe what they'll receive - or offers a vague promise of “news and special offers” - each subscriber will make his own assumption of what the email announcements will (or won't) include. By not setting expectations clearly, or by not meeting those that are set, marketers inadvertently cause people to delete their messages, unsubscribe from their list, or tag their mail as spam. Following this Best Practice is easy enough to start, but it requires good discipline to follow through.

Describe the topic, format, and frequency of the mailings you send

When creating an email sign-up form, publishers have a perfect opportunity to define their email newsletter or promotion to prospective subscribers. We recommend including brief text that describes the topics covered or type of content sent, the email formats offered, and the mailing frequency. For example, a publisher could indicate that subscribers will receive “a monthly, plaintext newsletter that discusses Issues A, B, and C.”

Likewise, a marketer could say that customers will receive “a weekly HTML alert of special, time-limited offers.” To further illustrate their cases, they could both link to previous mailings or samples of the type of content they distribute.

Reassure prospects about their privacy

As mentioned in Best Practice #1, the sign-up form is a critical place to reassure subscribers that you respect their privacy and the trust they show you by providing their email address. If you're using a double opt-in process, indicate on the sign-up form that new members should expect to receive a confirmation request; give them the email address it will come from, and suggest that they “white list” that address or domain. Next, make your organization's policy about email addresses readily available to prospective list members. Either as stand-alone text or within your larger privacy policy, be crystal clear about how you treat the email addresses and demographic information that list members provide you. Whether you use it internally only, share it with selected affiliates, or offer it to list brokers, let people know what they can expect. We also recommend that you explain to prospective list members that they may unsubscribe easily from your list - or be removed from your database, or otherwise stop receiving communications from you - at any time. The current CAN-SPAM legislation requires such unsubscribe instructions to be included within messages (see Best Practice #7), but you build additional good will and trust by explaining them upfront, before people actually submit their personal information to you.

Deliver what you say you will - not much more, and not much less

If you tell list members that you're going to send them a monthly text email with noncommercial content, don't send them weekly HTML messages with sales offers. Follow through with what you promised. And if you ask for personal information or preferences - for example, text or HTML email format - make sure you actually use it (in this example, send each group their requested format). If list members get something markedly different from what they expected, they'll likely be surprised, frustrated, or disappointed, and you'll miss your chance to build trust. In fact, you might even move the opposite direction and harm your organization's reputation. Also note that exceeding expectations isn't the only pitfall. If you've promised anything on a regular basis - certain content, delivery frequency, etc. - and then deliver less than that, you may also jeopardize your customer relationships. Anticipation of, and interest in, your next mailing may drop, or recipients may forget altogether that they'd heard from you previously. If you intend to send a monthly mailing, and then take a six-month break, be prepared for a surprised audience.

Watch out for negative feedback if you bend - or break - your habits

On occasion, you may find it necessary (or at least very tempting) to send content that doesn't fit your typical practice or subscribers' expectations. In these cases, proceed carefully and watch out for negative reactions; direct complaints will be obvious, but a higher than usual unsubscribe rate or lower than normal click-through rate may be signs that list members did not like your “special” message. In order to minimize fallout, we recommend that you preface your email with a clear indication of why you're sending the anomalous message; don't apologize for it, just present your rationale succinctly. A simple “We're sending all regular subscribers this one-time, special announcement about...” can preempt negative reactions - as long as you really mean “one time.” If you expect to send similar messages to your entire database in the future, the best practice is to let recipients know of your intended permanent change in advance.

Ask for topic and frequency preferences - and use them!

If you have a wide range of topics to discuss or offers to promote, or a very aggressive mailing schedule, consider offering subscribers a choice of what they want to receive and how often. You can then use the segmentation function of your email marketing tool to send specific content to the subscribers who've requested it. This approach helps prevent list burnout, and shows your list members that you recognize their personal interests.

BEST PRACTICE 3: TEST YOUR HTML FORMATTING

When you are preparing to send an email message using text and HTML versions, we highly recommend that you test your messages on multiple email clients before you send. This is because many people use many different email applications, similar to how many people use different browsers. (Just like there are multiple versions of Internet Explorer, Netscape, and Opera, etc., there are different kinds of applications people use to send and read email - for example, Eudora, Outlook, Hotmail, etc.) The Inbox Snapshot tool can help analyze your content in just this manner.

The reason to test your message on different email clients is that your message can render quite differently in each client. Some clients render the message nearly identical to how your message looked when it was designed and subsequently mailed. The change might be fairly insignificant, such as the background color and text color being switched. However, in other email clients, your message can look very different from how you intended it. For example, while some email clients can read HTML, they will not display graphics. As a matter of fact, these days, more and more email clients are hiding graphics by default, so make sure your message looks right with or without graphics. In some cases, HTML "alt" tags may be displayed even if the graphic is not,

so be sure to include them. As another example, AOL 9 will display a warning if HTML email messages contain images, prompting the recipient to select "yes" to open the message or "no" to skip the message. After clicking "yes", the HTML version will be displayed without images. (To view the images, the recipient will have to click another link for "show images & enable links".) Recently Microsoft released their latest version of Outlook, Outlook 2007, which breaks several features of HTML emails, specifically several CSS styles that allowed background images and advanced layouts. This break is also being applied to Hotmail. As a result, it is even more critical than ever to test how email content appears in these new email clients. Obviously, rendering differences can be quite varied. Depending on the extent of the changes in how your message renders, your message can simply look jumbled and disorganized, or it can actually be completely illegible. This is another reason why testing your email messages on multiple email clients is highly recommended!

BEST PRACTICE 4: OPTIMIZE FOR DELIVERY

Email content that looks great but doesn't actually reach its intended recipients can't be called successful. Best Practice #4 is to optimize your messages for successful delivery; a key issue in today's highly charged anti-spam climate. "Successful delivery" has a couple of different meanings; in this section, we describe critical first-tier efforts you can make to optimize your messages' chances of reaching your list members at all. In Best Practice #5, we cover second-tier actions you can take to help your messages get to recipients' inboxes.

Create good - complete and consistent - headers

The headers of your email messages are critical components for successful delivery. Some of the most important headers are the From, To, and Subject fields, all of which are scrutinized by automated anti-spam filters that protect ISPs and individual mailboxes. The human beings you're trying to reach also scan headers, of course.

First, it's very important to use a clear and consistent From header in each of your mailings. Use your organization's name and a valid email address, and then make sure you stick with that choice in each mailing; this consistency will help you encourage list members to "white list" your address, so your legitimate, opt-in mail will pass through successfully. If you want recipient replies to go to a different address than your From address, make sure the Reply To field is also valid.

Next, the industry standard is to include recipients' name and email address in the To field (e.g., "John Doe" <johndoe@example.com>). We enable marketers to customize the To field and insert the first and last name of the recipient if they so choose. Last, your subject line should be accurate and, ideally, compelling.

Accuracy is a key Best Practice; otherwise, you may appear to be intentionally deceptive and misleading. Compelling isn't necessarily a requirement, but it will certainly help increase the number of recipients who open your mail. Some list owners include a special Subject prefix for each mailing to increase the ease with which recipients may identify their messages (or to help aid passage through anti-spam filters). For example, the publisher of a daily foodservice newsletter could add the prefix "[The Daily Dish]" to the subject line so it can be readily identified in a recipient's inbox. If you distribute adult - oriented material, you may be legally required to include such a prefix to warn recipients of the content within. Headers are also a key mailing

component with which to experiment, for example, to determine which From address or Subject text is most effective at increasing your delivery or open rates; see Best Practice #8 for more about testing.

Write content that doesn't look like spam

As a legitimate, permission-based publisher or marketer, it's very likely that you have substantive content to share via email. That said, your mail can still appear to be spam if you inadvertently use certain words or formatting that's indicative of truly unsolicited email. These days, words such as "free", "mortgage", and "prescription" are so commonly used by spammers that your mail may be undifferentiated if you use them without caution. The Best Practice here is to create messages that have a good balance of text, graphics, and links, avoiding excessive use of words that are typically associated with spam. You might be able to gauge this on your own, but the true test is to...

Test your messages against spam filters

Use an online "content checker" that processes your draft message and then gives you a report of how it did against anti-spam rules. These tools often use a points system and score your message against a large number of rules. Every time your message triggers a rule, its assigned additional points; messages that accumulate more than a certain threshold of points are tagged as spam. The Content Analyzer tool will provide just such a check.

Adjust your headers and content to minimize chances of blockage

After you've run your test message through an anti-spam filter, edit your content to reduce definitive red flags. Note that some of your copy may have characteristics representative of spam, but it may not be worthwhile (or possible) to remove all of them. For example, if your business provides marketing consulting services, you may have no choice but to use the word "marketing" and accept the fact that some anti - spam filters may flag your mail because of it. (And if that's the only area of concern in your test messages, you likely have little to worry about!)

BEST PRACTICE 5: OPTIMIZE FOR THE INBOX

Once you've optimized your messages for general delivery - e.g., testing them with a content checking service to see how much they appear like spam - you're ready for the next step in fine-tuning. These days, many ISPs and mail providers offer their users a folder for mail deemed spam, junk, or otherwise "bulk." Unless your subscribers are diligent readers, they may simply delete mail that's automatically routed to these folders. You, therefore, want to do as much as possible to insure that your legitimate opt-in mail reaches the inbox.

Use test or “seed” addresses at key domains

First, see what domains are predominantly used by your audience, and get at least one address at the major ones. Most list owners have many members at Yahoo!, Hotmail, AOL, and MSN, but you may find others on your list. Sign up for at least one account at each of these providers, and then send your email campaign to yourself as part of your testing process. Make sure to use the same email marketing solution for this test that you'll use for your actual mailing in order to keep that important variable constant. The ISP Delivery Monitor tool can provide insight into the delivery to these ISPs.

BEST PRACTICE 6: CULTIVATE INDUSTRY RELATIONS

While it's tempting to see ISPs and other email providers as an obstacle between you and your target audience, they, like you, want to make sure that their subscribers receive legitimate opt-in email. Any ISP that didn't care about this and rejected too much valid mail would soon find itself losing customers. But unlike you, they also need to protect their subscribers from the current tidal wave of truly unsolicited, unwanted mail. As spammers get craftier, ISPs are forced to enforce stricter rules to filter out mail that looks like spam. Sometimes, despite your best efforts, it's your mail that gets filtered. How then do you make sure that your mail isn't designated a “false positive” on a regular basis?

Be sure you're missed

ISPs are in the business of delivering email people want - so make sure your email is something your customers want. When your message is interesting and relevant every time, recipients are unlikely to report it as spam to their ISPs. Indeed, if your customers look forward to receiving your email, they're more likely to miss it when it's not there and to let their ISP know they're unhappy that it's been blocked.

BEST PRACTICE 7: COMPLY WITH THE LAW

If you've sorted through the spam in your inbox and thought, “there ought to be a law,” you'll be glad to know that many countries now do have anti-spam legislation. (See <http://www.spamlaws.com> for more information.) Although the effectiveness of these laws in stopping spam has yet to be demonstrated, they have been effective in scaring many email publishers who are scared of breaking the law or of being sued. But if you're already following the Best Practices above, you'll find it's relatively easy to comply with the law.

Comply in six steps

The recommendations that follow are for email marketers in the United States and are based on the CANSPAM Act of 2003 (<http://www.spamlaws.com/federal/108s877.html>). It requires email publishers and marketers to comply with certain mailing guidelines:

- Don't “harvest” email addresses from the Internet or generate them via a “dictionary” process for commercial mailing purposes.
- Don't send commercial email via a computer that you don't have proper authorization to use.
- Don't falsify or obscure the header information in your commercial email messages; always use a valid From: address and an accurate, non-misleading Subject: line.
- Include a valid postal mailing address and a functioning opt-out mechanism in every commercial email message you send.
- Don't continue to send email to a recipient who has opted - out of your list.
- If you send adult content (i.e., sexually explicit material), use a warning label of that fact in your subject line.

As an ethical publisher or marketer, you're probably already following the provisions of the law; they're simply good practices, and we've discussed many of them in this document.

Don't forget your postal address

In our experience, the one step that many legitimate commercial senders have failed to adopt is the inclusion of their valid postal mailing address in every message they send. Insert this information into your standard unsubscribe footer and you'll be all set.

The law is important - but it's not everything

While laws like CAN-SPAM may not be very effective in stopping spam, they have helped email marketers think about their mailing practices; some are considering adopting a Best Practices approach for the very first time. But others have the mistaken impression that obeying the law is synonymous with ethical email marketing, and that's just not the case. You may alienate your customers, get your mail blocked, and tarnish your reputation if all you do is obey the law. That's just one part of your Master Practice.

BEST PRACTICE 8: ANALYZE RESULTS AND CLOSE THE LOOP

Many publishers and marketers are so busy that they don't make the time to analyze their campaigns to see what's working and what's not. They go by accepted wisdom for sending (e.g., mail on Tuesday, not on Monday) or use conventionally popular metrics to gauge their success (e.g., open and click-through rates). This final Best Practice advocates budgeting enough time and thought to identifying relevant success standards for your email publishing or marketing program and then using those insights to improve it.]

Identify key goals and associated metrics

It's hard to know if you've been successful if you haven't identified specific goals for your organization, as well as the relevant metrics for those goals. The first step is to think about why your organization is publishing an email newsletter or marketing via email. Is it to drive Web site traffic? Build sales? Generate advertising revenue? Inform users of new products? Demonstrate your authority in your field? The more concrete the goal, the more likely it will be that you will be able to prove you've achieved it. Once you've identified your goals, you can identify the metrics that will show whether you're meeting your objectives. Here are some examples:

- **Goal:** A professional organization is trying to increase attendance at its annual conference.
- **Metrics:** Subscriptions, colleague referrals, click-throughs on conference links (which topics are of most interest?), conversions.
- **Goal:** A consultant wants to demonstrate her expertise to a select clientele.
- **Metrics:** Click - through tracking, whitepaper downloads, conversions.
- **Goal:** A restaurant wants to promote business on its "dead" days to increase profits.
- **Metrics:** Coupon redemptions, location visits.

Benchmark your campaigns

Your first mailing or two will establish benchmarks for your chosen metrics. If you don't establish some initial reference points, it will be difficult to know if your campaigns are really generating desired results. The hypothetical restaurant owner above may think he's getting more business after sending a few campaigns and seeing full tables; but if he discovers that the increase in "dead day" business cuts into the rest of the week, he may simply be moving customers from full - price to discount nights. With benchmarks in hand, you can test different variables to see which creates better results. Pick one or two of the following, and watch your metrics carefully: Pitch, Offer, Formatting, Text/HTML, Time/day of publication, and Content/style.

Feed results back into subsequent campaigns

Success breeds success if you know what was successful. Once you've identified the key components of your email messages or the primary needs and wants of your audience, feed those insights back into your next campaign. Closing the loop from sending to receiving is what the Master Practice is all about, and in doing so you're both satisfying your list members and generating the results you want.

BEST PRACTICES: CONCLUSION

We tend to talk about the recipients of your mailings as a group, but each individual wants his or her personal preferences noted and respected. These Best Practices demonstrate your respect: your respect for privacy, your respect for preferences, and your respect for the privilege you've been granted to be allowed into the "privacy" of a person's inbox. Subscribers who are sent irrelevant mail too frequently will (rightly) feel the sender is at best careless and at worst contemptuous of their time - and trust. They may show their displeasure by unsubscribing.

Or, if they no longer trust the sender, they may choose to stop the mail by deleting it, blocking it, or by reporting it as spam to their ISPs. When you follow these Best Practices - really they are Expected Practices - when your email is requested, interesting and valuable, recipients will tend to open and act on it. It's more likely to be delivered and received in their inboxes, too. And you'll stay in good standing with the law. Your recipients are judging the value of your messages every time they receive one, so don't get complacent. Conduct regular reviews to be sure you are continuing to follow these Expected Practices, and as the Internet continues to evolve, be sure you adopt the new Best Practices that will surely follow and possibly improve upon those we've outlined here. Your audience's inbox is a crowded place these days, but by following these

Expected Practices and the overarching Master Practice, your email is more likely to be welcome and even much - anticipated.

HEADQUARTERS

Redi-Mail Direct Marketing
5 Audrey Place
Fairfield, NJ 07004
Phone 973.808.4500
Fax 973.808.5511
Email sales@redimail.com

20 Gloria Lane
Fairfield, NJ 07004
Phone 973.808.4500
Fax 973.808.5511

AFFILIATES

Redi-Data, Inc.
10 New Maple Avenue
Pine Brook, NJ 07058
Phone 877.288.3282
Fax 973.227.4069
Email sales@redidata.com
redidata.com

4577 Nob Hill Road
Suite 209
Sunrise, FL 33351
Phone 877.288.3282
Fax 954.835.2903

Dialog Marketing Services, Inc.
Healthcare Dialog
10 New Maple Avenue
Pine Brook, NJ 07058
Phone 973.461.2980
Fax 973.227.4069
Email sales@dialogmktg.com
Email sales@healthcaredialog.com
dialogmarketingservices.com
healthcaredialog.com

StayinFront, Inc.
107 Little Falls Road
Fairfield, NJ 07004
Phone 973.461.4800
Fax 973.461.4801
Email sales@stayinfront.com
stayinfront.com

healthcaredialog.com

sales@healthcaredialog.com