RIGHT NOW®

BEST PRACTICES

Email Deliverability

Optimizing delivery and participation rates with RightNow Marketing and RightNow Feedback

Web address: http://rightnow.com

Email address: info@rightnow.com

Introduction

Even the most carefully designed and targeted mailing is subject to external hazards that can interfere with its delivery. Due to the vast amount of spam transmitted each day and the aggressive systems used by consumers to combat it, legitimate business emails are sometimes filtered without notice. Organizations that do not convey a good-faith intention to engage in ethical mail practices are at risk of being blacklisted by Internet Service Providers (ISPs) and email-reputation management services. And even mail that is successfully delivered may be ignored by the recipient or reported as spam.

Though most of these challenges stem from factors beyond the creation and delivery of mail, RightNow Technologies goes to great lengths to help you overcome them. RightNow vigorously protects the integrity of our hosted mail domains and aligns our services with the latest industry-accepted practices and technologies promoting the efficient delivery of email to consumers. However, as a RightNow user, it is equally important that you follow certain guidelines to ensure you receive the best possible return on your marketing efforts.

The recommendations in this document can help you achieve excellent delivery and conversion rates for mailings and surveys. They have been field-tested over millions of deliveries by some of the world's largest companies using RightNow. While best practices alone will not guarantee that your email will always be accepted, these suggestions will greatly improve the likelihood that your messages will be delivered to and viewed by your intended recipients.

Note This document refers to functionality and features available in RightNow Marketing and RightNow Feedback, but does not contain instructions for their use. For information and step-by-step procedures, refer to the *RightNow Marketing User Manual* and the *RightNow Feedback User Manual*.

In this document

What is deliverability?

The recommendations in this guide will help you attain your most important goal: increasing message deliverability. But what *is* deliverability?

Deliverability is the degree to which an email message aligns with industry-accepted practices to ensure delivery to an intended recipient. It reflects your ability to communicate your message to your contacts with minimal interference. Emails with "low deliverability" are often blocked by ISPs and spam filters, whereas emails with "high deliverability" are more likely to result in optimal audience participation and conversion rates. Put simply, deliverability translates to increased efficiency and success.

Three major factors influence the deliverability of your messages: your reputation, your audience, and your content. The following sections will help you manage these factors effectively.

Protecting your reputation

Ultimately, your ability to deliver messages to your contacts is a direct reflection of your organization's reputation as a responsible Internet citizen. Just as a credit limit depends on the borrower's credit reputation, your ability to successfully send mass mailings depends on your reputation for adhering to industry best practices for email delivery. If you don't follow those practices faithfully, you risk having your communications blocked across large swaths of the Internet. Therefore, as you spend time and money creating an effective mailing strategy, it is important to protect that investment by establishing a positive reputation with ISPs and content monitors.

Use a "warming" process for new IP addresses

Leading ISPs and deliverability services closely monitor addresses sending mail to their servers, especially those they have not seen before. Volume and consistency are evaluated over 30-day periods, and reputations are established based on senders' adherence to acceptable practices. When implementing a new dedicated IP address, it is critical that you use a warming process to start building a good reputation.

A warming process consists of segmenting your high-volume mailings into smaller batches to ensure a moderate message load. For example, if you want to send your first mailing to a list of 200,000 contacts, you should segment the audience and send to 15-30,000 contacts at a time over a period of several days. It is also important that your initial mailings reflect industry standards for managing contacts and content, as described in this document.

Done correctly, the warming process will indicate to all who are monitoring your activity that your intentions are honorable and that you do not intend to blast the Internet with spam. Establishing this level of trust is critical for ensuring the success of your bulk mailings.

Implement a complaint resolution process

To ensure clean contact lists and prompt follow-up of legitimate customer replies, be sure to implement a plan for handling questions, out-of-office responses, and unsubscribe requests. Regularly monitor administration accounts, such as abuse@yourdomain.com or postmaster@yourdomain.com, and honor all abuse complaints as unsubscribe requests.

Monitor ISP deliverability

The deliverability policies of leading ISPs and email services change frequently. Closely monitor policy updates so you can react to changes appropriately. It is also useful to create a "seed list" of accounts with the major email providers (such as Hotmail, Yahoo, Gmail, and AOL) to test the deliverability of your mailings. You can also work with a RightNow referral partner to monitor delivery and rendering of the mail you send to those email providers.

Implement authentication

Organizations that send mailings from branded domains should implement email authentication to protect their reputations and secure delivery rates. RightNow supports two forms of authentication.

- **Sender Policy Framework/Sender ID**—Sender Policy Framework (SPF) and Sender ID are email authentication options that designate permitted senders of email originating from your domain, excluding those with mismatched or incorrectly specified SPF/Sender ID records. For information about implementing SPF or Sender ID, refer to Answer ID 2489 on our RightNow support site.
- **DomainKeys/DomainKeys Identified Mail**—DomainKeys (DK) and DomainKeys Identified Mail (DKIM) are email authentication options that use cryptographic signatures to designate email as originating from an authorized email delivery provider, excluding messages sent from those with unsigned or incorrectly assigned signatures. For information about implementing DomainKeys or DKIM, refer to Answer ID 2701 on our RightNow support site.

Honoring your audience

Organizations are often challenged to communicate effectively with prospects and customers through the unique medium of email, where the rules of the road vary greatly from more traditional forms of advertising. Fatigued by the volume and persistence of spam, today's consumers have little patience for even legitimate business communications that don't reflect their interests. Conversely, an organization that honors the time and interests of its customers and prospects can sustain interest and inspire loyalty for the duration of the relationship.

The following strategies can help your organization develop sustained, trusting relationships with your contacts.

Avoid purchased mailing lists

One common myth is that the larger your audience, the more likely your mailing is to be successful. In reality, the success of a mailing depends more on the quality of the contacts in your list than the quantity. Sending email indiscriminately to people who may have no interest in your product or service can do much more harm than good, landing you on blacklists and ruining your reputation.

The quality of purchased lists cannot be easily verified and is often poor. Email address turnover is common and frequent. Services may claim that their lists are current and appropriate for your needs, but there is no practical way for you to confirm this. Some disreputable list providers obtain their email addresses by tricking consumers into thinking they have won valuable prizes, or by sending out web spiders (link-following scripts) to scour the Internet and harvest contact information found on web pages—behavior that hardly inspires trust and loyalty. To protect their customers from such tactics, ISPs often seed those lists with "spam trap" email addresses that don't belong to anyone. If an email is received by a spam trap address, the ISP will regard the message as spam and blacklist or penalize the reputation of the sender.

As you can see, the battle against spam is complex and the danger to marketers is clear. If you are not certain about how your contacts were obtained, you risk undermining your reputation among major ISPs across the Internet.

Fortunately, the most successful strategy is also the most ethical: develop your list yourself. Obtain contact data from your company's consumer touch points, such as advertisements, trade shows, web sites, message boards, trainings, conferences, and customer service requests. Encourage these contacts to share their interests with you through surveys or contact profile settings. Deliverability increases significantly when the contacts in your database are not only active but also keenly aware of you and interested in what you have to say. And after all, isn't that the point?

Obtain opt-in permission

Among the tools you can use to assess the interests of your contacts, opt-ins provide the clearest indication. By "opting in" (explicitly granting permission to include them in communications), your contacts are affirming not only interest but trust in your organization. And for most companies, nothing is more valuable than a trusting customer relationship.

There are two common opt-in methods.

- **Single opt-in**—A contact submits an email address (usually from a web form) and indicates a willingness to receive communications from you. The system sets a contact opt-in field to Yes. Explicit contact permission has been granted, but no additional effort is taken to confirm that the person who submitted the email address is the owner of the email address.
- **Double opt-in**—Sometimes referred to as a confirmed or closed loop opt-in. A contact submits an email address and indicates a willingness to receive communications from you. Then, to ensure the email address was actually submitted by its owner, you send a confirmation request to the address. The contact responds positively to the email (usually by clicking a link) to confirm interest, and a contact opt-in field is set to Yes.

When soliciting opt-ins from your contacts, it helps to clarify what kind of information they are agreeing to receive. At each opt-in location, provide a brief summary of the content and frequency of the messages you will be sending. By spelling out the conditions under which you will contact them, you will set the right expectations and ensure that contacts sign up to receive only messages that interest them. When you send a mailing, RightNow makes it easy for you to honor those expectations by using opt-in fields to segment your audience.

For information about creating opt-in custom fields, refer to the *RightNow Administrator Manual*.

Include a gentle reminder

Your contacts have busy lives with many distractions. It is not uncommon for someone to opt into a mailing list and then, a few weeks later, forget doing so. To reduce the risk that your contacts will begin rejecting messages that they once agreed to receive, add a small reminder that they are receiving your messages because they opted in. Briefly mention the conditions under which you are contacting them and lightly touch on the value they are receiving. Contacts will often be more receptive to your messages if they remember agreeing to receive them and, more precisely, *why*.

Use single-click unsubscribe

Another important way to inspire trust is to include an unsubscribe link that allows a contact to opt out of all communications with a single click. In other words, you should *not* require contacts to log in or provide additional information in order to opt out globally.

Why would you want to make it easy for contacts to opt out of your meticulously compiled mailing list? Because it is required by U.S. law. And if you don't, recipients could report you to their ISP by simply clicking a "mark as spam" button in their mail client. Customers can be fickle about mailing lists; even if they previously opted in, they often take the most convenient route to opt out. Providing an unsubscribe link is a legal requirement, but it is simple to do and helps protect your reputation and avoid annoying your valued prospects and customers.

Link to your privacy policy

With the prevalence of spam and advent of identity fraud, consumers are wary of sharing personal contact information, and rightly so. You can give your customers peace of mind by inserting a link to a privacy policy explaining how their profile information will be used. A strong privacy policy assures contacts that their information will not be rented or sold to a third party unless they explicitly opt in to a partner email promotion. Stating this information in explicit detail can remove lingering privacy concerns and build additional trust and goodwill into your relationship.

Promote addition to address books

Another helpful strategy is to ask contacts to add your email address to their address book. Most mail programs will refrain from tagging mail as spam or routing it for deletion if the sender's address is listed in the address book. This simple step both reaffirms your contacts' interest and promotes consistent delivery of your messages to their inbox.

Review invalid email addresses

Initially, one might not feel concerned about sending to a list that contains a few invalid email addresses. After all, does it really matter if you get a few bounce messages back from each mailing?

Yes, it matters. In reality, including invalid email addresses in mailings can eventually become an expensive proposition. Because it costs money to store data and send bulk email, a large number of invalid email addresses can add up to a substantial sum. More importantly, they will decrease your viewing and conversion rates. In addition, sending regularly to email addresses that are known to be invalid can hurt your reputation.

To help mitigate these risks, RightNow can automatically process bounce notifications and, when appropriate, mark contact addresses as invalid so they are excluded from future mailings. RightNow can also automatically revalidate contacts that were disabled but later found to be valid. For more information about the processes used to manage invalid contacts, refer to the *RightNow Administrator Manual*.

RightNow provides reports that monitor bounce messages and invalid contacts, and it is a good idea to check these after every mailing. If you find a high percentage of bounces or invalid addresses per mailing, you may need to reevaluate your audience acquisition and list maintenance practices. In addition, the Invalid Email Address Domains report displays a list of contact email addresses from well-known domains that contain common typographical errors (such as "htomail.com" instead of "hotmail.com"). For information about using reports, refer to the *RightNow Analytics Manual*.

Producing well-formed content

Once you have navigated your message through the pitfalls of reputation management and spam filtering and into the inbox of a contact with whom you have carefully established a relationship, you are home free, right?

Not quite. Most often, your message will be buried among several others of varying priority. Your contact may click on your email just briefly, evaluating its importance next to messages from family and friends, a daily horoscope, a newsletter, and perhaps even a few notes from other companies pitching products of their own. Clearly your work does not stop at getting your message into a friendly inbox—to be successful, your email must attract your contact's attention.

So how do you produce well-formed content that clearly delivers your message without looking like spam? Here are several proven strategies for designing consumer-friendly communications.

Stand out in the inbox

Most mail clients list new messages by From address, subject, and time received. If you want your message to be opened, the content in these fields is key. If it isn't clear who you are or what you want, your message can easily be passed over.

Refine your message subject to be concise yet informative. Make sure it clearly states your purpose and any special conditions of your offer. Also, use easily identifiable From and Reply To addresses to help recipients recognize your organization as the sender. And be sure you don't include special (non-alphanumeric) characters, as they can falsely lead filters to believe that the email is spam.

Add deliverability features as snippets

Snippets are a convenient way to ensure that key deliverability features are included in every mailing. Snippets can be used for elements such as your mailing address, a copyright reference, a link to your company web site, a privacy policy link, an unsubscribe link, an add-to-address book request, and reply instructions (if different than replying to the Reply To email address).

As previously described, these elements are essential to keeping trust with your contacts. Some are even legally required (see "Complying with CAN-SPAM laws" on page 10). Providing these elements as snippets can make it easier to remember to include them.

Avoid content associated with spam

Whether based on simple rules or complex algorithms, systems designed to filter spam can sometimes screen out perfectly legitimate business communications. This is because they sift through passing email for specific triggers; that is, characteristics or bits of content commonly associated with spam. If the content of an email contains a spam trigger, the message could be bounced or blocked and the sender's reputation could suffer.

During the proofing process, be sure to screen your content for potential spam triggers. When composing or proofing your messages, be sure you do not use all caps, special characters, excessive punctuation, or certain words and phrases. Refer to Table 1 for a list of potential spam triggers.

Table 1: Phrases Associated With Spam

50% Off	Don't Delete	Order Now
100% Free	Discount	Opportunity
Act Now	Double Your Income	Promise You
All New	Earn $$$	Please Read
Amazing	Easy Terms	Requested

Table 1: Phrases Associated With Spam (Continued)

As Seen On	Excessive $ or !	Subscribe Now
Buy Direct	E.X.T.R.A. Punctuation	Special Promotion
Cash Bonus	Free	Save Up To
Call Now	Join Millions	Satisfaction Guaranteed
Credit	Million Dollars	Serious Cash
Compare	No Cost	You've Been Selected
Collect	Now Only	Why Pay More

Do not include email attachments

Virus scanners and spam filters often block emails with attachments. Also, large attachments can clog recipient inboxes and impair mail delivery. As an alternative, RightNow Marketing enables you to include a file link in your message instead. Using a file link instead of attaching a file gives your contacts the option to download and view the file while making the message less prone to filtering.

Test all messages appropriately

Before launching your mailing, make sure to test it thoroughly. Send proof copies to yourself and your team to proof the spelling, layout, embedded links, and accuracy of the content. Also be sure that all content (including the design, offers, copyright, and legal disclaimer information) has been approved by your legal and marketing teams, and other appropriate management.

Once proofing is complete and you are ready to launch, use RightNow's market testing feature to send your mailing to a randomly selected subset of your audience. Market testing enables you to test your mailing's effectiveness using real contacts, so you can identify any last-minute issues before to launching to your entire audience. Market testing can also be used to test different versions of a document with varying content or subject text to optimize your message for maximum return.

Share communications internally

Make sure that all contact "touch points" (groups in your organization that work directly with customers) are aware of all high-volume communications being sent. Share a sample of each mailing to promote awareness across your customer support, sales, and marketing functions. Providing a consistent message across all channels increases customer loyalty and improves satisfaction.

Monitor campaign effectiveness

Once you launch your mailing, monitor its performance by analyzing standard reports to track delivery and participation rates. Measure campaign effectiveness by tracking completion actions such as purchases, downloads, or form submittals.

Complying with CAN-SPAM laws

Because legal definitions and penalties for spam vary among countries, it is vital that you closely monitor current and pending laws that marketers are required to follow when sending commercial emails. One important example of such legislation is the CAN-SPAM Act of 2003.

The CAN-SPAM Act of 2003 includes the following requirements.

- Email must not contain false or misleading header information.
- Email must not contain a deceptive subject line.
- Email containing advertising content must be identified in the subject line.
- Email containing adult content must be identified in the subject line.
- Email must include the sender's physical mailing address displayed in ASCII text.
- Email must include a way for recipients to easily opt out of all lists, not just the list used to send the message in question.
- Email must not be sent to contacts who have previously opted out. All opt-out requests must be processed within 10 days.
- Email must not be sent to harvested or generated email addresses.
- Email must not be sent to domains in the FCC (Federal Communications Commission) wireless list.

RightNow helps you conform to CAN-SPAM laws by providing a checklist of key provisions. When creating a mailing or survey with an invitation message, RightNow automatically checks that the message contains a physical address and an unsubscribe link, and that the message honors global opt-in preferences.

In addition, RightNow helps you track whether certain requirements passed or failed. However, you must track these items manually.

- **Verify that the message uses a candid subject line.** CAN-SPAM compliance requires that the subject line of an email accurately reflects its contents. To pass this requirement, make sure that the subject line is not deceptive to the email recipient.
- **Verify that the subject identifies adult content in the message.** The CAN-SPAM act requires that a message containing adult content must contain the text "SEXUALLY EXPLICIT" in the subject line of the email.
- **Verify that the subject identifies the message as an advertisement, when applicable.** The CAN-SPAM act requires that the message contains clear and conspicuous notice that the message is an advertisement or solicitation. To pass this requirement, make sure that the subject line accurately reflects the message's content.
- **Verify that the From and Reply-To headers contain accurate information.** CAN-SPAM compliance requires that the From and Reply-To headers and routing information, including the originating name and email address, accurately identify your organization.
- **Verify that you are not sending to harvested or generated addresses.** Harvested email addresses are gathered randomly from web sites or web services by indexing scripts. Generated email addresses are formed using a "dictionary attack," by combining names, letters, or numbers into multiple permutations.
- **Verify that you are not sending to email addresses that contain domains in the FCC wireless list.** The CAN-SPAM act prohibits the sending of messages to wireless devices, such as mobile phones. The FCC publishes a list of domain names used by cellular companies that you can download at http://www.fcc.gov/cgb/policy/DomainNameDownload.html.

Important The checklist available in RightNow is used to determine compliance with some key provisions of the CAN-SPAM Act of 2003. You should use this information in conjunction with and not as replacement for legal counsel. For information about the CAN-SPAM laws, refer to the Federal Trade Commission web site at http://www.ftc.gov/spam. Other sites that can help you stay current with the law include http://www.spamlaws.com and http://www.findlaw.com.

Glossary

Abuse complaint—An email from a consumer to an ISP or organization indicating spam has been received. Abuse complaint emails are often addressed to abuse@<yourdomain>.com or postmaster@<yourdomain>.com.

Authentication—A process used to confirm someone's identity, such as the sender of an email.

Blacklist—A list of email senders that have been blocked by ISPs or spam filter services for sending spam. The best way to avoid being blacklisted is to maintain a positive reputation.

See Reputation.

Bounce notification—An error message (often classified as "hard" or "soft") returned from a recipient's mail server when it is unable to deliver an email to the designated address. A soft bounce indicates the error is temporary (try again later), whereas a hard bounce indicates that the error that is unlikely to be resolved.

Branded domain—An Internet domain name associated with a specific organization.

CAN-SPAM Act of 2003—U.S. legislation governing commercial email communications, regulated by the Federal Trade Commission. CAN-SPAM laws apply to all commercial email sent to addresses hosted in the United States.

Confirmed opt-in—*See* Double Opt-In.

Deliverability—The degree to which an email message aligns with industry-accepted practices to ensure delivery to an intended recipient. Emails with low deliverability are often blocked by ISPs and spam filters.

Domain name—The unique name of a server or service on the Internet (such as a web site or mail server), commonly associated with an IP address. In an email address, the domain name usually follows the @ symbol.

DomainKeys (DK)—A form of email authentication that uses a cryptographic signature to verify that an email message originated from a specific organization. DomainKeys differs from DKIM authentication primarily by the email headers used to generate the signature.

DomainKeys Identified Mail (DKIM)—A form of email authentication that uses a cryptographic signature to verify that an email message originated from a specific organization. DKIM differs from DomainKeys authentication primarily by the email headers used to generate the signature.

Double opt-in—A verification process that ensures an opt-in request originated from the owner of the submitted email address. Sometimes referred to as Confirmed Opt-In.

See also Opt-In.

From address—In an email message, the field containing the email address of the message sender.

Greylisting—A method used by ISPs to protect their customers from spam by initially rejecting messages received from unrecognized senders, but accepting them on the second try. Most spammers do not attempt to send an email more than once if the first try is rejected.

IP address—The unique network address of a server or service on the Internet, often associated with a domain name. ISPs and email authentication services often track the reputations of mail servers by IP address.

Internet service provider (ISP)—A company that provides web and/or email services. Examples of leading ISPs include Yahoo, AOL, Hotmail, Qwest, and Comcast.

Opt-in—The explicit granting of permission by a contact to receive email communications from an organization. Opt-ins may be specific to certain mailing lists, or applied globally across all mailing lists. Sometimes referred to as Single Opt-In.

See also Double Opt-In.

Opt-out—An explicit request by a contact to be removed from a specific mailing list or from all lists, most often communicated by email or web form. Also referred to as Unsubscribe.

Privacy policy—A document that clearly defines how an organization may use the contact information stored in its database, published for the benefit of consumers.

Reputation—The degree to which a sender of mass email has been known to adhere to industry-accepted practices for email delivery, as monitored by ISPs and deliverability services. A positive reputation can improve a sender's delivery rate; a negative reputation can lead ISPs to block mailings from the sender's IP address.

Response rate—The number of emails receiving a positive response as compared to the total number of emails sent. An example of a positive response would be the clicking of a tracked link in the email; a simple viewing of the email would not be considered a response.

Sender ID—A form of email authentication that identifies IP addresses authorized to send mail on behalf of a specific organization. Sender ID differs from SPF authentication primarily by the components of the email used to authenticate the message.

Sender Policy Framework (SPF)—A form of email authentication that identifies IP addresses authorized to send mail on behalf of a specific organization. SPF differs from Sender ID authentication primarily by the components of the email used to authenticate the message.

Single opt-in—*See* Opt-In.

Spam—Any email that is considered to be unwanted and/or unsolicited by the recipient.

Spam trap—A special email address created by an ISP for seeding into mailing lists used by spammers. ISPs use spam traps to detect and block mail from known spammers to protect consumers.

Template—A base document design commonly consisting of headers, footers, logos, and deliverability elements. Templates can be applied to documents to save time and ensure a consistent design across multiple mailings.

Test cell—A special set of email addresses used to receive proofs and test the deliverability and rendering of mailings.

Unsubscribe—*See* Opt-Out.

Warming—The process used to establish a good reputation for a new IP address among ISPs and content monitors. The warming process typically includes sending initial mailings in batches and strictly adhering to industry best practices.

See Reputation.

Whitelist—A list of email senders permitted to send email to one or more customers of an ISP.