



Email Data Management Best Practices

September 17, 2008

These Best Practices have been developed by the IAB Email Committee.

About the IAB Email Committee:

The Email Committee is dedicated to removing friction from the email marketing channel, increasing its use by marketers and publishers, and solidifying its place in the marketing mix. The committee works to recommend solutions, standards, best practices and educational tools to the industry as needed.

A full list of committee member companies can be found at:

http://www.iab.net/member_center/35088?iabid=a0330000000rZ45AAE

This document can be found on the IAB website at: <http://www.iab.net/emaildata>

IAB Contact Information:

Ryan Walker

Manager of Industry Services, IAB

212-380-4731

ryan@iab.net

Table of Contents

Executive Summary	3
Permission and Use	4
Licensing Data to List Managers.....	5
Marketers Renting Third-party Email Lists.....	5
Techniques to Improve Inbox Deliverability	7
Authentication	7
Accreditation	7
Reputation.....	8
Protecting and Improving Reputation Score.....	Error! Bookmark not defined.
Defining Responsibilities	11
Data Security and Sharing of Suppression Files.....	12
Unsubscribe Best Practices	13
Data Append Best Practices	16

Executive Summary

Email marketing professionals from the IAB's Email Committee developed these Best Practices to remove friction from the email marketing channel by simplifying the core elements of security, deliverability, permission and privacy. This document concerns the practices and systems that responsible parties of the email marketing ecosystem should adhere to.

It is the committee's belief that adherence to these best practices will:

- Increase the likelihood of email deliverability and therefore campaign performance
- Promote Consumer and Advertiser trust in and adoption of the email channel
- Encourage responsible practices by all involved in the email ecosystem

This document outlines recommendations for several key data topics related to email marketing and is intended for publishers, marketers and service providers. These best practices were developed by thoroughly examining several of the most critical issues surrounding the email marketing industry, including privacy, permission, data security, and deliverability. Key best practices include:

- Senders should only send commercial email to individuals who have provided informed consent
- For all third-party licensed data, a global unsubscribe mechanism should be implemented
- Consumer permission to receive commercial email from a List Owner cannot be replicated or transferred without reference to the original point of collection
- Clear, conspicuous and repeated notice of data collection and use are required
- Advertisers and marketers should authenticate their email by publicly registering the domains from which they send email
- Anyone using email for marketing purposes should adopt and use authentication protocols for both their email and corporate domains
- All parties should use a one-way encrypted hash to encrypt suppression files

The general belief of the Email Committee is that by developing clear data management guidance the industry will increase consumer trust in the medium. The IAB is confident that, if adopted, these Best Practices will protect consumers while improving the overall quality and performance of email marketing campaigns.

Permission and Use

In the context of email marketing, permission refers to an individual's informed consent to receive commercial email. Permission may be extended to a marketer alone, or to a marketer and its third-party marketing partners, depending upon the language utilized at the point of collection.

Email Senders and their Email Service Providers should only send commercial email to individuals who have provided informed consent. The IAB Email Marketing Pledge acknowledges the critical importance of consumer consent to email marketing. The Pledge outlines the levels of consent that are supported by the IAB. Please note that proper consent must be gained prior to conducting any email marketing efforts (To review the entire Email Marketing Pledge, please visit: http://www.iab.net/iab_products_and_industry_services/1421/1443/1458/79222). Email senders should also have procedures for tracking consumer communications preferences, and provide readily accessible privacy policy links on the origination page where informed consent was obtained from the consumer.

- ❖ Many companies that build email address lists (List Owners) are not experts on the complexities of monetizing that email list through advertising. Accordingly, these companies often contract with third-party List Managers with a core competency in monetizing email lists through advertising. If List Owners share email addresses with List Managers for monetization purposes, significant due diligence procedures is necessary to validate the third parties' compliance with CAN-SPAM and ensure adequate protection of the data. It is recommended that List Owners use a seeding regime and other procedures as more fully described in the section; "Data Security and Sharing of Suppression Files".
- ❖ Consumer permission to receive Commercial Email from a List Owner cannot be replicated or transferred without reference to the original point of collection.

All email sent by a List Owner or List Manager should clearly inform the consumer about the original permission source, and provide the consumer with a means to revoke that permission. This can be accomplished through various means, such as adding the following language to the bottom of the email: "You are receiving this message because on <Date> at <Time> <Email Address> registered to receive marketing messages from <website> and its marketing partners. To change your marketing preferences with <website>, go to the website and select <Name of the link> to review your options."

- ❖ Once the consumer has revoked their permission, all email from senders that use that point of permission must discontinue sending future email to that consumer.
- ❖ It should be noted that higher levels of consent will likely increase open and deliverability rates and reduce consumer complaints.
- ❖ Advertisers should not use email addresses collected through surreptitious or misleading methods such as dictionary attacks or harvesting.
- ❖ Advertisers should perform due diligence with third parties to understand their data collection procedures and build into contracts prohibitions against non-consent-based collection and safeguards to create accountability on their data collection practices.

Proper permission should be obtained prior to conducting any email campaigns and consumers' subsequent requests to revoke that permission should be honored by all senders relying upon that point of consent. In addition to benefitting consumers, higher levels of permission should benefit marketers by increasing deliverability and open rates, reducing "Report Spam" complaints, and improving marketers' relationships with consumers.

Licensing Data to List Managers

This section refers to situations where a List Owner licenses their permission-based list to a third-party List Manager. In addition to requiring a List Manager to contractually adhere to CAN-SPAM compliance and other applicable laws, the IAB Email committee also recommends the following best practices:

- ❖ **From Line:** The From Line should always indicate the name of the Sender as defined under CAN-SPAM.
- ❖ **Subject Line:** The Subject Line should indicate the subject matter of the email message, such that a reasonable person would not be surprised. It is not a requirement, nor is it recommended to use the word “Advertisement” or any variation of the term in the subject line. If the word “Free” is used in the Subject Line, and the product being advertised is not genuinely free, then a clear disclaimer should be included in the Subject Line.
- ❖ **Header:** Header information (source, destination and routing information) should not be false, deceptive or misleading.
- ❖ **Content:** List Owners should specify which content areas are appropriate and which are inappropriate (i.e. no alcohol or tobacco offers to a list of teens).
- ❖ **Data Security:** The List Manager should implement and maintain appropriate safeguards to protect and secure the list and immediately notify the List Owner in the event of a breach. All best practices in the “Data Security and Sharing of Suppression Files” section of this document should be adhered to by the List Manager.
- ❖ **Opt-Out Requests:** The List Manager should honor all opt-out requests as soon as notified by the Sender, or immediately if the List Manager is the Sender. List Managers should not require any information beyond a consumer’s email address or any other obligation as a condition for accepting or honoring a consumer’s opt-out request, including but not limited to requiring a consumer to visit more than a single Web page.
- ❖ **Transparency:** The List Manager should publicly register the domains from which it sends email. List Managers should also provide the WHOIS database with their accurate name, physical postal address and telephone number, such that the domain name in the “from” and “reply-to” headers of each email identify the List Manager via a WHOIS database search. The List Manager must not use WHOIS Guard or a similar technology which masks the identity of a sender.
- ❖ **Audit:** The List Owner should retain the right to regularly audit the List Manager’s use of the list.
- ❖ **Penalties:** The List Manager should be penalized for using or sharing the list in violation of its agreement with the List Owner.

Marketers Renting Third-party Email Lists

Email list rental can be one of the most effective forms of direct marketing available to marketers. Yet it is fraught with risk, and requires tremendous expertise in order to generate successful return on advertising spending. Finding the right partner is often not enough; marketers must also be diligent in considering various email list rental programs. There are generally three types of partners that marketers can choose to partner with. All three may offer more extensive services similar to a traditional agency:

:

- List Brokers; do not own or manage data themselves, but their expertise is in choosing the right lists and selections.

IAB Email Data Management Best Practices

- List Managers; represent a specific set of lists in the market. Their expertise is in designing a successful program across their managed lists.
- List Owners; as the name suggests, own their list(s). Their expertise is specific to the lists that they own.

Regardless of which partner they choose, Marketers should also perform due diligence on all new lists before renting them. This due diligence should at least include collecting the following information:

1. Information about the Website or location of data and permission collection, including but not limited to URL, privacy policy, number of daily page views, and content.
2. Contact information, including but not limited to name, telephone number, fax number, email address, and mailing address.
3. Payment information, including payee name, address, telephone number, and type, tax ID, and social security number.
4. IP addresses should be verified, and run through a third-party reputation monitoring service such as SenderScore.org.
5. Evidence validating their compliance with CAN-SPAM.

Additionally, Marketers should maintain strict licensing controls and procedures for any data exchange. These procedures and controls can include any or all of the following:

1. Using a revocable license form of contract
2. Seeding of lists
3. Ensuring that consumer unsubscribe requests are honored

Techniques to Improve Inbox Deliverability

Email marketers care about performance. Performance can be measured in many ways, including response, relevance, ROI, clicks, opens, etc. What is becoming increasingly clear to all email marketers, regardless of how they measure performance, is that the ability to deliver messages successfully to the recipient's inbox plays a critical role.

The IAB Email Committee recommends the following techniques be employed by email marketers to improve inbox delivery and ultimately performance:

Authentication

Authentication is a cost-free, interoperable and easy way to guard against phishing and spoofing attacks. Authentication also increases the likelihood that emails will be delivered to the intended recipient and into their inbox. The IAB Email Committee strongly recommends that anyone using email for marketing purposes adopt and use authentication protocols for both their email and corporate domains.

- ❖ There are two prevailing and complementary authentication systems available to advertisers:
 - Sender-ID Framework (SIDF)/Sender Policy Framework (SPF)
 - Domain Keys-Identified Mail (DKIM)

The IAB Email Committee recommends advertisers adopt both authentication systems.

- ❖ The IAB Email Committee joins the Authentication & Online Trust Alliance (AOTA), as well as other prominent groups, in issuing a call for compliance of all consumer-facing e-commerce and online brand sites to adopt one or more forms of outbound email authentication for their top-level corporate domain by 2009. It is critical to consumer trust that the many companies who have adopted authentication for their marketing sub domains, also focus on consumer and brand protection by authenticating their top-level corporate domains.
- ❖ The IAB Email Committee calls on all ISPs to implement inbound email authentication verification, in addition to existing messaging hygiene solutions, to maximize consumer and brand protection by 2009. This commitment by the entire interactive ecosystem is required to preserve trust and confidence in both email and e-commerce.

In summary, the IAB Email Committee strongly recommends that anyone using email for marketing purposes adopt and use both Sender ID and Domain Keys authentication protocols for both their email and corporate domains. Marketers however cannot solve this problem alone; ISPs and ESPs must implement inbound authentication verification practices. Together we can protect legitimate brands and their customers.

Accreditation

In addition to allowing users to block specific email senders, most ISPs partner with spam filtering companies with the goal of blocking unwanted email that displays characteristics of spam. Sender accreditation refers to a third-party process of verifying email senders and requiring them to adhere to accredited usage guidelines in exchange for being listed in a trusted listing that ISPs reference to allow certain email to bypass email filters. These lists use similar technology as block lists, but improve delivery from legitimate commercial senders.

- ❖ Registration of new websites or transfers of any existing site to a new domain registrar should include consideration of whether the registrar supports authentication protocols
 - Compliance with email authentication standards requires the ability to create and publish DNS TXT records. Many businesses get their DNS hosting services from a domain registrar or other third-party provider. If your DNS provider does not support TXT records, you will not be able to comply with email authentication standards.
 - We recommend contacting your DNS service provider or your domain registrar to ask if they offer support for email authentication standards, specifically including publishing DNS TXT records.
- ❖ Review the list of providers that do support TXT records ¹
- ❖ Work with the IT team to authenticate corporate level domain and any email communication sub-domains:
 - For more information on SenderID and SPF, review the following links:
<http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx>
<http://spf.pobox.com/>
 - For more information on DomainKeys, review the following link:
<http://antispam.yahoo.com/domainkeys>
- ❖ Use this link to see if the domain is already registered:
<http://senderid.espcoalition.org/>

Reputation

A sender's email reputation is determined by email recipients, ISPs, and other email monitoring organizations. ISPs rely on these collective opinions to determine reputation scores. The reputation score of a sender is a critical factor in determining whether ISPs choose to deliver their email to the inbox, the bulk folder, or not at all.

- ❖ Each ISP uses different data sets and algorithms to determine a reputation score; however, some major factors are consistent. They include:
 - i. Recipient complaints
 - ii. Unknown email addresses
 - iii. Spam traps
 - iv. Authentication
- ❖ ISPs and their service providers apply different filtering to incoming email according to the reputation score of the sender.
- ❖ Most Major ISPs offer whitelisting services for legitimate bulk email senders. It is recommended that email senders participate in these programs. Each ISP has a unique application process for whitelisting. Generally, mailers will need to provide details related to the opt-in/opt-out policies and demonstrate a history of being a responsible email sender.
- ❖ Several major ISPs offer feedback loops as a mechanism for mailers to remove complainers from their lists. Most ISPs provide complaint data to senders to facilitate the removal process. It is recommended that Spam Complaints received from feedback loops be treated as unsubscribe

¹ <http://www.aotalliance.org/resources/index.html>.

requests. Additionally, complaint data should be used to evaluate and identify possible problematic campaigns.

A more complete list of places to find feedback loops can be found at:

- ReputationWiki.org:
http://reputationwiki.org/~reputati/index.php?title=Feedback_Loops
- Datran Media's whitepaper:
http://success.datranmedia.com/whitepaper/feedbackLoop_whitepaper.pdf

Protecting and Improving Reputation Score

As previously stated, reputation scores have a serious impact on deliverability. The IAB Email Committee has developed the following list of techniques to protect and improve reputation scores.

❖ Prohibit BCC

No commercial sender should send commercial email through any system that uses the cc or bcc field. There are too many opportunities for error if you are not using a mailing system that actually creates a separate message for each recipient, with only that recipient's unique qualifying information it. Even the best companies can have processes go awry; therefore it is best to disallow using the CC or the BCC to send mass commercial emails. An example of this process breakdown is the FTC's settlement with Ely Lilly in 2002 for emailing 600 Prozac customers and accidentally including those 600 patients in the CC field instead of the BCC field.

❖ Delivery Monitoring

Senders should monitor total delivery as well as inbox delivery. Total delivery can be measured by the difference between the number of messages sent and the number of bounced messages. While this method will not provide a good indication of what messages customers are seeing, as messages may be sent to junk folders, it will provide a good metric to be used in evaluating list hygiene.

Inbox delivery is much more difficult to measure and is much more valuable than true delivery. There is no fully accurate way of measuring true inbox delivery at this time. The best method to get a reasonably accurate measure of inbox delivery is by setting up seed accounts for each of the major ISPs and monitoring those seed accounts.

Mailers are also urged to evaluate click and open data by domain. A low click or open rate for a particular domain may be a good indication that the email was sent to junk folders.

❖ Hygiene

Hygiene is the process of making sure your email list is accurate and up-to-date. This means removing addresses that have unsubscribed or are undeliverable for any reason. It also includes having good opt-in and opt-out processes so your subscribers can help you maintain the integrity of your database. Monitor the age of your database. Additionally, establish an on-going process for actively removing subscribers that are both old and inactive. Allow subscribers to easily change their email address on file with you – and use a consumer-reported Email Change of Address (ECO) service on a quarterly or semi-annual basis.

❖ Address Collection and Permission

- Be clear about what you are offering the consumer. State the benefits, the content of the emails, the frequency and when the subscriber should expect the first email.
- Keep permission current. Reach out to subsets of your file who are not opening or clicking every quarter or so. Ask if they would like to receive something different, or provide feedback on your email program.
- Your address collection or hygiene process should reject or remove malformed addresses (i.e. me@hotmail.com).
- Your address collection or hygiene process should reject or remove abuse@ and postmaster@ addresses.
- Your address collection or hygiene process should reject or remove role accounts (i.e. sales@company.com, customerservice@company.com).
- Your address collection or hygiene process should reject or remove email addresses containing profanity.
- Provide an email preference center for easy updating of email addresses.

❖ Bounce handling

Email bounces are automatically generated messages that are sent from an ISP in response to an undeliverable message. Different email servers reply in different formats for the bounces they send back.

The major types of bounces are:

1. **Hard bounces:** A hard bounce indicates that an email cannot be delivered due to a permanent error (i.e. a mailbox that does not exist). Hard bounces should be removed immediately from a list or after a small number of consecutive hard bounces.
2. **Soft bounces:** A soft bounce is generated when an email cannot be delivered to an address due to a temporary error. A soft bounce indicates that it may be possible to deliver to the address at some point in the future. If an address bounces continuously for a period of time, it is recommended that senders remove the address from their lists.
3. **Blocks:** ISPs send bounce messages sometimes with a reason code describing why the mail was blocked. Senders have to make sure that these are handled differently from bounces and work with the ISPs to remove these blocks. The risk of not isolating these blocks is that legitimate email addresses would otherwise be tagged as bounces and removed from the list.

Since different email servers reply in different formats, senders are encouraged to work with technology providers or have their own proprietary technology to translate and categorize the different kinds of bounce codes. The technology should also be able to provide automated processes to enforce bounce handling rules. If internal reporting is available, unknown user rates should be monitored by campaign, by data source, and by sending IP.

❖ Variable Envelope Return Path (VERP)

1. Senders are recommended to implement VERP (technique to enable automatic detection and removal of undeliverable email addresses) or one of its variants for handling bounces. There are instances where ISPs do not include the original message or email address as part of the bounce message. Senders have to ensure that they have some other mechanism to identify the bounced address other than relying on the ISP to provide the email address.
2. It is recommended that senders closely monitor and manage bounce rates.
3. A common question is how email senders can reactivate addresses removed due to bounces. It is recommended that senders do not reactivate hard-bounced addresses unless emails were misclassified as bounces. Reactivating old hard-bounced addresses can cause deliverability problems since many ISPs use inactive addresses as spam traps.

❖ Partner Vetting and Auditing

If you receive subscriptions from third-party partners, affiliates, or list services:

1. Be sure to vet potential data partners. Choose partners with good reputations and compliant sending practices.
2. Test a sample of the file from a separate IP space and monitor Unknown User rates before adding the file to your database.
3. Review the partner data file to ensure that you are not receiving malformed addresses or role account addresses.
4. Mail partners from separate IP space to monitor their on-going data quality and Unknown User rates.
5. Regularly audit your partner's sign-up process to ensure that it meets industry best practices for address collection.

Defining Responsibilities

Although the roles and responsibilities of the initiators and senders of commercial email are established by CAN-SPAM, it is prudent to reiterate and further define these roles and responsibilities in a written contract governing the email marketing relationship. The contract should address all key business and legal terms of the relationship, including but not limited to:

- The terms of the license, the services to be provided,
- The obligations of each party,
- Data security,
- Restrictions on data usage and email content,
- Suppression,
- Compliance,
- Compliance monitoring,
- Term/termination,
- Reporting,
- Payment,
- Representations and warranties,
- And indemnification.

Data Security and Sharing of Suppression Files

We recommend that senders should use a one-way encrypted hash to encrypt suppression files that are shared with third parties that send on the sender's behalf, or a third-party bonded mail house as the preferred method for sharing suppression lists between advertisers and publishers for the protection of consumers.

In addition, we recommend that advertisers seed the suppression files used by their publishers on a regular basis to validate proper usage.

❖ **One-way encrypted hash:** There are many one-way encrypted hash algorithms, though the most prevalent today is MD5. Obviously this is safer than distributing the email addresses in plain text because it prevents against human error, accidents, theft and fraud. By using MD5 instead of plain text, advertisers can be confident that their unsubscribe list will not be accidentally sent an email message, will not be easily exposed to a third-party, and will not be stolen or abused without malicious intent. SHA-256 should be the eventual replacement for MD5.

❖ **Third-party Bonded Mail House:**

A third-party bonded mail house is an independent entity that can take a sender's suppression list and a third party's mailing list, and "scrub" one list against the other, giving the third party a copy of their mailing list ready to be used, without revealing the sender's suppression list's contents. Senders should use a neutral, bonded, third-party mail house to scrub a third party's mailing list against the suppression list. Some benefits of third-party cleansing are:

- There is an audit trail, showing the proper use of the suppression list.
- Whole domain suppression is usually easier to perform for all parties (i.e. the sender wants to suppress all @domain.com email addresses).
- Super-suppression is possible (i.e. suppress bob@yahoo.com across multiple third-party mailers, so that bob@yahoo.com only gets one email from the advertiser per campaign or per week).
- Advertisers can include "active customer lists" in their suppression lists, further reducing customer service costs associated with invalid offers reaching current customers.

❖ **Suppression list management and sharing for publishers and advertisers:**

Publishers: When sending mail on behalf of a third-party advertiser, that advertiser must be asked for their suppression list, if the advertiser is the sender. If provided either in hashed format or through a third-party bonded mail house, the publisher's mailing list should then be scrubbed against the advertiser's suppression list before the offer is sent, ensuring that people who have opted-out of that advertiser's messages don't receive the promotional message a maximum 10 days before the mailing will be sent.

Advertisers: When sending mail to a consumer through a third-party publisher, the publisher should be provided a way to scrub its mailing list against the suppression list, if the advertiser is the sender.

In summary, suppression list abuse is a major issue affecting the industry. Any party that needs to share a suppression list with a third-party should do so securely to protect the value of the inbox over the long-term.

Unsubscribe Best Practices

The CAN-SPAM Act of 2003 and its update in 2008 provide requirements for senders² of commercial email. However, we recommend that marketers consider going beyond those compliance requirements by implementing the following best practices:

❖ **Provide clear links or instructions to unsubscribe.**

It is critical that unsubscribe placements are prominent and have clear, definitive language. The unsubscribe should be included in all email types such as advertisements, newsletters, alerts, customer service responses, forward to a friend or other viral campaigns, even though CAN-SPAM only requires opt-out language on “commercial messages.” Marketers should evaluate transactional message unsubscribes depending on their business processes and the primary intent of the message.

• **Sample Language:**

The IAB’s examples of acceptable language are “Click Here to Unsubscribe”, “Remove me”, and “Unsubscribe”. It is illegal under CAN-SPAM to require users to log-in to an account with a username and password to unsubscribe, or to require anything other than the entering of an email address to unsubscribe.

❖ **Make it easy to change email address.**

If you want to include other options in the email you are sending such as an option to change an email address, the link should be clearly labeled as such. An example of acceptable language would be “Change email address”.

❖ **Users should be given a Web-based and email-based mechanism for unsubscribing.**

When possible, marketers should allow users to unsubscribe through a Web-based mechanism (for example, “click here to unsubscribe” leading to a Web page) or an email-based unsubscribe mechanism (for example, “Reply to this message with ‘Unsubscribe’ in the subject line”). Mobile device users may only be able to reply to your email. Users that have email forwarded from another account may only be able to click a link to a Web page. At a minimum, marketers that solely utilize a Web-based mechanism must have a system in place that informs users who attempt to unsubscribe by replying to the email that such requests will not be honored and reiterates the Web-based option.

❖ **Unsubscribe requests should be processed immediately.**

It is best to process a user initiated unsubscribe request immediately. CAN-SPAM requires the sender to honor all unsubscribe or opt-out requests within ten (10) business days of their receipt.

² The “sender” as defined by CAN-SPAM is required to collect an unsubscribe or opt-out request. CAN-SPAM must be understood to be all commercial email senders, and understanding how “sender” is defined is imperative when applying that definition to all mail sent by the List Owner, on behalf of others, or when others send on the Owner’s behalf.

❖ **Unsubscribe mechanisms should be tested.**

Because senders are legally required to provide an opt-out option that works for 30 days after the email is sent, it is important that senders consistently check their unsubscribe system to ensure it is working. Sudden changes in data such as lower unsubscribe rates can be an indicator that the mechanism is not processing unsubscribes. If possible, a third-party should be hired or internal audit procedures implemented to test unsubscribe mechanisms, even if a third-party ESP service is already being used. This will enable a way to provide further evidence of CAN-SPAM compliance, and alert parties of potential problems.

❖ **Offer users the opportunity to unsubscribe from all email sent by that same line of business or division.**

A line of business or division may provide users with a menu or newsletter-specific opt-out instructions; as long as the menu or choices offered to the consumer include the option of being removed from all newsletters within that line of business or division.

❖ **Honor unsubscribe requests across all similar lines of business within the organization.**

If a user unsubscribes from a commercial email sent by one line of business or division, that request should be honored across all similar lines of business or divisions within a given organization, unless the email that was sent offers line of business or division specific opt-out instructions. The opt-out rate can be lowered by offering multiple options that allow users to opt-out of specific messages by brand or by offering. Lines of business or divisions are similar if a reasonable consumer could conclude that they are identical.

❖ **Sender vs. third-party mailer unsubscribe**

In third-party marketing emails (where an advertiser has contracted with a List Owner or manager to send an offer on the advertiser's behalf to consumers through the third-party), the Sender is required to collect unsubscribes and honor them in the future. The best way for a Sender to do this is to provide their own unsubscribe URL for the third-party mailer to include in the email. The third-party mailer might also want to include their own unsubscribe link in the email if they conclude they are a Sender also. However, this may confuse users that want to discontinue receiving email from the Sender but not from the third-party mailer. Furthermore:

- CAN-SPAM now allows for multiple senders to “designate” one sender where there are multiple products and services being advertised or promoted, but it is important to note that that part of the law is optional, and that if the designated sender fails to comply with CAN-SPAM in any way, all senders in that message may be held liable for non-compliance with the law.
- If there are multiple unsubscribe options in an email, the unsubscribe URLs should be clearly marked (i.e. “Click here to unsubscribe from future offers from ADVERTISER” and “Click here to unsubscribe from PUBLISHER”).

❖ **Postal address display**

CAN-SPAM requires a postal address in commercial email. Senders should use the postal address that will be checked for unsubscribe requests as the postal address in commercial email sent on their behalf. When there are multiple senders and the marketers have not designated one of the entities as the “CAN-SPAM designated sender” in accordance with the law, it should be clear which postal address is associated with each sender.

❖ **Global unsubscribe**

If you license your data to third parties, a global unsubscribe mechanism is recommended. All companies should honor unsubscribes throughout the life cycle of the email address. If a company shares a consumer's email address with third parties for marketing purposes, then that company should provide a global removal mechanism on their website and in the emails sent out by their contracted third parties. The company should have adequate resources and systems in place with all contracted third parties to ensure all parties mailing the email address have received and utilized the global removal file in a timely manner. Companies using third parties to deploy email should also have internal seeding procedures in place to validate compliance and usage of the global removal file by contracted third-parties. These procedures will ensure that consumers are globally removed from all commercial email efforts that originated from that company.

If a company does not have adequate infrastructure to perform these described tasks, including the global opt-out functionality on the website, the company should contract with all third parties to deliver any preference information submitted by consumers regarding opting out of future email communications. The company then should process that information and redistribute updated email lists in a timely fashion.

Data Append Best Practices

Data append is a useful practice that helps marketers maximize the value of their customer databases by; enabling them to more effectively target customers, provide more relevant messages, keep customer records current, lower the cost and increase the efficiency of communicating with customers. There are two situations involving email addresses in which a marketer may wish to use Data Append techniques to enhance its database of consumer information. They are:

❖ **Appending PII and/or Non-PII to Email Addresses**

Many marketers have a database of customer email addresses they would like to enhance by appending personally identifiable information (“PII”), such as full name, postal address and telephone number. Marketers may also desire to enhance their database of consumer email addresses by appending non-personally identifiable information (“Non-PII”), such as gender, age, demographic information, and lifestyle statistics. In order for a marketer to append PII or Non-PII to their database of customer email addresses, the privacy policies under which the email addresses were collected, as well as the privacy policies under which the data points to be appended were collected, must allow for the practice.

- ❖ Marketers should contractually obligate 3rd party Data Append providers to ensure that data being appended was collected with proper notification of such use within their privacy policy

❖ **Appending Email Addresses to Customer Records**

Email Append is the process of adding a consumer’s email address to that consumer’s record in a marketer’s database. Appending email addresses to existing customer records requires special care. If this tactic is employed, marketers should be aware of an important risk; that your brand’s reputation with your customers and Internet Service Providers may suffer. The IAB Email Committee recommends that marketer’s approach this tactic with caution.

1. A best practice when employing email append is to ask permission from your customers to email them.
2. Have the 3rd party data provider send the email to your customers on your behalf.
3. Send the permission request emails in small batches, test response, and optimize performance.
4. We strongly recommended that you use Opt-In as the method of asking permission from your customers.
5. Extra effort and cost should be applied to ensure the correct email address has been appended to the correct customer record. Avoid household level matches in the case of multi-person households.

In order for a marketer to append email addresses to existing customer records, the privacy policies under which the existing consumer data points were collected, as well as the privacy policies under which the email addresses to be appended were collected, must allow for the practice.

Data appending offers many benefits to marketers. A proper and successful append process is contingent upon the use of a reputable data provider and the procurement of the proper level of permission from the impacted consumers. When these two elements are combined, consumers benefit, as well.