



Best Practices:
Email Marketing strategies for 2008

Date: January 2008

CONTENTS

Introduction	3
Methodology	3
Can-Spam Act	4
Email Address Data Collection	6
Message Distribution	9
Viral Email Marketing	10
Response Tracking	11
Conclusion	12

Introduction

In the days before the mass acceptance of the World Wide Web, email existed merely as a communication tool utilized by the educated elite within government and research academics. Less than a decade later, email has evolved into the fastest growing communication medium ever seen by man. In 1995, less than 5% of the United States adult population regularly used email. By the close of 2006, Gartner Group predicts that this usage will reach nearly 65% and span all socioeconomic and demographic strata. Email acceptance has now greatly outpaced the adoption of telephone technology in the early twenty first century.

The advertising community has also embraced email. Specifically, for its potential as a cost effective commercial direct marketing tool. This entire field of email direct marketing barely existed five years ago but today represents a \$4 billion industry. Forrester Research predicts the email marketing industry to reach \$6.6 billion in total expenditures by 2008.

This tremendously rapid growth, combined with the relative infancy state of the industry, create a situation where the players are developing, and changing, the “rules of the game” on seemingly a daily basis. The players include: industry trade groups, consumer activist groups, and recently legislative groups. The “rules of the game” involve some of the most basic issues of direct marketing and a philosophical struggle between who holds the power to control this new medium. Is it the sender? The recipient? Or possibly the deliverer?

While the field of email marketing continues to evolve, large opportunity remains for those players that understand the current issues and how to best respond. With that in mind, this *Best Practices: Permission Email Marketing* document was created as a guide representing the latest in thought leadership from Boca Networks.

Methodology

This Best Practices white paper combines input from the follow sources:

- The Direct Marketing Association and the Association for Interactive Media. Specifically, the “6 Resolutions for Responsible Emailers created by the Council for Responsible Email and published June 2000.
- Current consumer trends. Recent public statements from recognized leading consumer protection groups such as the Center for Democracy and Technology, Electronic Privacy Information Center, Mail Abuse Prevention System, and the Spam Recycling Center.
- A pragmatic Customer Value Management approach (e-CVM). Best practices must

ultimately be oriented around effective financial business management. The recommendations presented in this white paper all facilitate industry ethics, consumer needs, legal restrictions, AND create profitable email marketing.

This document organizes *Best Practices* into four sections based on the chronology of the email marketing process. That process begins with data collection, i.e. email address data collection. Best Practices in email data collection revolve around the issues of gaining, verifying, and documenting permission.

Can-Spam Act

AN OVERVIEW AND COMPLIANCE.

We finally have a national law to replace a patchwork quilt of state legislations that attempted to deal with spam. Regardless of whether you feel CAN-SPAM isn't strong enough or relieved it's replaced that onerous California law, it *is* law now. You have to deal with it, so we'll focus on how to deal with its key points.

CAN-SPAM's biggest impact will be on advertisers who obtain much or all of their leads and customers from third parties or affiliates, when those affiliates use e-mail. We've heard through the grapevine several advertisers are putting controls into place to ensure affiliate managers and their networks will comply with the law. Some are canceling any and all e-mail promotions until these practices are in place and a court of law determines fine points concerning unsubscribes.

We must balance compliance so we don't eradicate the ability to acquire new customers with e-mail. We also don't want to overreact as we attempt to better define a new e-mail playing field. Meanwhile, bear in mind CAN-SPAM holds advertisers liable, along with all parties involved in sending e-mail. Everyone in the e-mail chain must toe the line.

Control is key. The last thing an advertiser needs is an affiliate sending e-mail that violates the law. The advertiser may not even know about it. Most likely, advertisers, affiliate managers and other companies will develop affiliate guidelines. Affiliates will be required to sign off on these, and fail-safes will be put into place.

During this period, e-mail volume will likely drop for legitimate e-mail marketers, and all entities in the e-mail chain (advertiser, affiliate, agency, service bureau, Web sites, email list owners, etc.) will see revenues dip. Hopefully, it won't last long. (The law won't affect true e-mail abusers, against whom it was written).

Compliance is also key in this new era. Advertisers must ensure rules and processes required for affiliates are followed. If you're an advertiser, you may want to work with your promotional

partners to ensure the following components of the law are upheld:

Header falsification. One way to police this, and other no-noes under the new law, is to seed the lists of all affiliates who mail your offers. Checking e-mail you receive is an easy way to spot falsification.

Misleading subject lines. It's standard practice among many advertisers: Ensure you clearly state emailers can only use approved subject lines, copy, and graphics. You can easily monitor this from your seeded addresses.

Unsubscribe process. The law requires e-mailers remove within 10 days anyone who unsubscribes. You can review seeded e-mail to make sure an unsubscribe link is present and working.

There's a gray area in this requirement. Say an advertiser and an affiliate emailer both maintain a database, and someone unsubscribes from a mailing sent by the e-mailer on behalf of the advertiser. It's not 100 percent clear if the unsubscribe request must be honored for both advertiser and e-mailer, or if the request pertains only to the e-mailer's database. A court may need to decide.

If you interpret this to mean someone unsubscribing must be removed from both databases, it creates a logistical nightmare. Imagine this scenario:

Advertiser A, with its own prospect and customer database, use affiliates A, B, C, D, and E. Affiliate A owns four different databases. All the affiliates mail the advertiser's offer; 1,389 people unsubscribe from affiliate A's database. Does this mean Affiliate A must provide those e-mail addresses to the advertiser, who in turn must remove them from its own database? Must it also send the addresses to every affiliate it has and require them to remove the addresses from any databases they have?

Obviously that scenario could never work. It isn't worth the tremendous time and effort to implement such a system. So what do you do? After lots of discussion with advertisers and others, the most sensible long-term (but currently impractical) approach is to unsubscribe people from both the e-mailer's list and the advertiser's database whenever possible. Keep an electronic record for proof.

Going further than this is overkill. If a consumer opts in to an offer from multiple sources, they deserve to get e-mail from multiple sources. The larger point is all affiliates should honor unsubscribe requests and be able to provide proof upon request.

Notice the e-mail is a solicitation. A clear notification that a message is commercial is required, but you don't have to place a conspicuous "ADV" in the subject line. From a marketing perspective, we recommend incorporating the following in the attribution line:

You are receiving this advertisement because you requested information from [the advertiser or list owner].

Valid postal address. This shouldn't be a problem for any legit marketer. Include a real postal address where consumers can contact you. Time will tell if this is the advertiser's or the list owner's.

We appointed a compliance officer at Boca Networks. I suggest you do the same. Though legitimate marketers strive to utilize "best practices," you must now make sure your best practices are in line with the new legislation.

Email Address Data Collection

ALWAYS USE PERMISSION MARKETING TECHNIQUES.

All industry organizations, consumer groups, and even some governments, mandate that advertisers utilize commercial email only in a permission mode. This means that the marketer must gain permission of the recipient prior to emailing.

True permission contains complete and honest disclosure. No trickery, deception, or half truths. True permission goes beyond just a simple, small font, disclosure to mean that the recipient actually understands that he has given permission.

For example, a marketer could completely and honestly disclose that by entering a sweepstakes you thereby give permission to receive email ads. But what if that disclosure was made in small print buried in the Privacy Statement? Yes, the marketer complied with a disclosure requirement but did the recipient truly understand? Probably not.

This permission requirement pertains not just to prospects but also current customers or other parties with whom a business relationship already exists. From a legal and industry standards point of view, most statutes do not require additional permission when a prior business relationship exists. However, from a successful email marketing perspective, Boca Networks recommends gaining permission even from current customers.

Rationale – Gaining permission requires considerable effort, time, and money, so why bother? Many marketers say, “If they don’t like receiving my email they can just hit delete or Unsubscribe. Plus, we don’t need permission before sending direct postal mail. Why with email?”

Here’s why.

- *It's the law:* Not everywhere but many states require permission or a previous business relationship to send an email ad.

- *Customer service nightmare:* Mailing unsolicited spam email will 100% guarantee a flood of hate reply mail. A flood of reply hate mail following a spam campaign has crashed dozens of companies' websites and internal mail systems. Plus, for a brand name company, such a flood of hate reply often leads to negative publicity.

- *Loss of Your Internet Service Provider:* Nearly all ISPs terminate service to customers they believe send non-permission commercial email. In addition, an Internet watchdog group called MAPS (Mail Abuse Prevention Service) will blacklist any company they believe conducts nonpermission based email marketing. Nearly 2,000 ISPs use the MAPS, Spamhaus or SpamCop Blacklist, which can cause up to 40% of the marketers outbound email to go undelivered. This mail does not "bounce" back. Rather, the participating ISPs simply choose to filter and not deliver the email to their subscribers.

NEVER "HARVEST" EMAIL ADDRESSES.

Harvest means to collect email addresses, without the owner's consent. Typically accomplished via scanning chat rooms, bulletin boards, web pages, directories, or any other publicly available source. Spammers harvest email addresses by the millions everyday.

Rationale – Harvesting email addresses violates the previous Best Practice. While this technique can certainly generate huge email prospect databases at extremely low cost, the ROI is negative. Harvested email lists typically generate clickthrough rates of less than 0.01%. (1,000,000 harvested addresses would produce less than 100 clickthroughs) However, the customer service, legal, and negative publicity costs far outweigh any revenue generated.

AVOID THE USE OF "MUST FILL" FIELDS.

"Must fill" means that the user must enter his email address into the field in order to complete the data entry on a web page. The "submit" button will not activate until the user completes all "must fill" fields. Seems odd not to require the one basic field needed to conduct all email permission marketing. However, permission marketing centers on the notion of the consumer having control, and deciding whether or not to give data. Permission marketing removes control from the advertiser and makes techniques that enable the marketer to "take" data less effective.

Rationale – The use of "must fill" fields often results in the collection of garbage data. For example, the marketer ultimately collects a database with addresses such as: bob@bob.com, mickey@mouse.com, ihateyou@spammer.com. Most of these addresses generate bounced, undeliverable email and a waste of both time and money. However, some of these garbage addresses may be valid but to a different user. For example, bob@bob.com. Bob may become quite upset and accuse the marketer of spamming when he receives an email ad.

ALWAYS SEND A CONFIRMATION AUTORESPONDER EMAIL. OPT-IN CONFIRMATION IS PREFERABLE.

After the user submits his email address the marketing should immediately trigger back an autoresponder email, which confirms the user's registration. The marketer can format this confirmation message as either an "opt-in" or "opt-out."

An opt-out confirmation informs the user that their submission was received and added to the database. If the user wishes not to be added to the database the message includes instructions on how to terminate or "opt-out" – usually a "reply" or a URL hyperlink. If the user takes no action from the confirmation email, they are then automatically added to the marketer's database. Hence, do nothing and the registrant receives email ads.

An opt-in confirmation informs the user that their submission was received but their email address will not be added to the database until the user actively confirms their initial opt-in. Typically the user confirms by either a reply or clicking on a URL in the email. Hence, do nothing and the registrant does not receive any email ads.

Rationale – A confirmation email removes the risk of a forged or accidental registration. Confirmation enables a potential registrant to stop the campaign before it starts in case of an error or if they've simply changed their mind. Confirmation emails are not required by law or even by marketing industry standards. However, most every consumer protection group advocates confirmation emails as a best practice for email marketing.

Hence, employing such a technique will build public goodwill.

Additionally, confirmation auto reply also helps to improve overall database quality. In permission marketing, quality far outweighs quantity in importance. Utilizing an opt-out confirmation auto responder will result in a loss of 5%-10% of registrations. Utilizing an opt-in confirmation will result in a loss of up to 40% of initial registrations. A significant drop-off but for long term, customer value management, Boca Networks recommends an opt-in confirmation as a Best Practice.

ALWAYS LOG THE DATE, TIME, AND IP LOCATION OF EACH EMAIL ADDRESS COLLECTED.

Marketers should always log the time, date, and IP address of every email address collected via their permission email submission page. In addition, collection of the date and time that the Confirmation autoresponder was sent should be collected. Even better best practice is to collect the date, time, IP address, when the user opts-in again via the opt-in confirmation message.

Rationale – Simply put, people forget. People will sign-up for an email list and later completely forget. When the marketing email arrives they often claim no knowledge and accuse the marketer of spamming. Obviously, this places the marketer in a defensive position. A permission audit trail immediately resolves the issue. If the user avails himself of legal action this audit trail data can prove extremely valuable.

Message Distribution

NEVER FALSIFY THE SENDER HEADER INFORMATION.

Header information includes the domain, IP address, and any other routing information that enables a user to determine the origin of the email. Sender routing information may be redirected to enable a 3rd party processor to physically broadcast the message but that redirected routing must maintain a traceable path to the message origin.

Rationale – Spammers forge their message headers in order to avoid detection by upset consumers and law enforcement authorities. Legitimate permission marketers want their messages to plainly appear as credible and not spam. Hence, clear and accurate headers are a basic ethical and legal requirement for email marketing and with the passing of the Can-Spam act is now the law.

NEVER FALSIFY THE SUBJECT LINE.

The basic “truth in advertising” doctrine applies. An advertiser can certainly employ effective “teaser” copy within the subject line but not intentionally fraudulent information. In addition, never use tactics intended to mislead the reader about the expected content. For example, do not use RE: or FW: in the subject to mislead the reader into believing this message is connected to a previous communication with another party. Also, do not use subject line phrases intended to convey a previous friendship relationship when in fact none exists; for example “Hi”.

Rationale – Falsified, misleading, and deceptive subject lines remain the hallmark of spam. Even the most novice Internet user can immediately recognize and delete Spam messages. Hence, legitimate email marketers should design their messages to appear as distinctly non-spam as possible. The first step is a clear “From” address and header. Second, is a credible subject line.

ALWAYS INCLUDE AN EASY UNSUBSCRIBE OPTION.

Every commercial email message must include a mechanism for registrants to unsubscribe from the mailing program. The unsubscribe process may be implemented via a simple “reply” or via a URL link to an unsubscribe page. Regardless of the method, each and every outbound commercial email must include an unsubscribe option.

Rationale – Every state, federal law, and the Direct Marketing Association all mandate that marketers include an unsubscribe option on every outbound message. Penalties for not providing an unsubscribe option range from civil to criminal with fines up to \$500 per nonconforming message.

ALWAYS HONOR UNSUBSCRIBE REQUESTS BEFORE RE-MAILING.

Providing an unsubscribe mechanism remains a primary and mandatory requirement for email marketers. However, providing that mechanism means nothing if the marketer fails to honor the unsubscribe request before the next mailing. Hence, if the marketer does not maintain a system which enables real-time database (mailing list) update of unsubscribe requests, then the frequency of database unsubscribe updates will dictate the maximum frequency at which the marketer may mail.

Rationale – Managing unsubscribe requests remains the most important database hygiene issue for email marketers and one of the most important aspects of permission marketing for consumers. As stated previously, the penalties for not properly managing unsubscribe requests can be litigious and expensive.

Viral Email Marketing

ALWAYS INCLUDE REFERRER NAME.

The virally generated message should include, either in the “From” address or in the subject line, the name of the person that requested the message be forwarded. As stated previously, all outbound email marketing messages must include accurate sender and header information. In the case of viral email marketing there exists two senders: 1) the original email marketer, and 2) the referee that requested the message be resent. The recipient must be informed of both senders.

Rationale – Without the referee’s name, the recipient will assume that the email message was sent directly from the marketer and without permission. Many viral email campaigns backfire because the recipient misperceives the message as a spam. This misperception not only leads to unsuccessful viral marketing but can also lead to litigation.

IMPLEMENT SAFEGUARDS TO PREVENT SPAMMER HIJACKING.

Viral programs risk hijack by spammers when either of the following conditions exist.

- A monetary, cash, or other real payment for each viral prospect submitted.
- Unprotected email server technology.

In the case of a cash reward, spammers will use the marketer’s viral offer and mail, i.e. spam, to potentially million of recipients. Viral incentives should be limited to free information, purchase discounts, or free product with the purchase of product. Direct cash payment, as often used in multilevel marketing, creates tremendous potential risk of abuse. In the case of unprotected

server technology, spammers will use the viral program as a means to launch their own spam campaigns undetected but traceable back to the viral marketing company.

Rationale – In the case of hijacking, the spammer incurs the civil and potentially criminal legal exposure. Typically, the unwitting viral marketer remains an innocent bystander. However, from a public perception point of view the marketer is guilty. Several very large, brand name companies have fallen victim to spammers hijacking their viral programs.

PERMISSION IS NOT TRANSFERABLE.

Email addresses submitted by referees do not become permission addresses for future use by the marketer. The temptation to load these email addresses into the marketers permission database is large; however, every industry and consumer group strongly advocate against this practice.

Rationale – Simply stated, reusing virally submitted email addresses is not a permission marketing practice. All of the rationale stated previously concerning utilizing only permission tactics fully applies.

ALWAYS LOG THE DATE, TIME, AND IP LOCATION.

Best practice recommends that the viral marketer log the date, time, and IP location of each referee participating in the program. In addition, the viral marketer should also log the date and time of the email addresses submitted by the referee.

Rationale – In the event that the viral program becomes hijacked by a spammer, or simply accused of promoting spam, the marketing should maintain this data as an audit trail to defend against such charges.

Response Tracking

PROVIDE FULL DISCLOSURE AND AN OPT-OUT.

As a best practice, marketers should disclose within their privacy policy any individual level tracking the marketer conducts. This includes uniquely coded URLs for individual click-through tracking, “cookies”, “bugs”, or any other implanted coding techniques that enable a marketer to track an individual’s web behavior from the starting point of an email marketing message.

Rationale – This disclosure is not currently mandated by law or by any marketing industry groups. However, numerous consumer protection groups are highly energized on this issue. Best

practice to proactively disclose these tracking practices rather than be “exposed” and placed into a defensive position.

ALWAYS LOG THE DATE, TIME, AND IP LOCATION OF EACH CLICK-THROUGH.

The great power of web marketing, and email marketing in particular, is its trackability. A marketer can measure every message sent, every click-through generated, and track those results back to the individual registrants.

Rationale – To blindly email market without measurement and tracking rarely generates a maximum return on investment. Measuring at the campaign level (total messages sent, total clickthroughs, etc.) provides a first level of refinement and an increase in return on investment. Second level involves tracking results back to individual registrants and utilizing that information to develop modeling and true Customer Value Management.

Conclusion

The recommendations outlined in this document serve as operating guidelines for Boca Networks concerning email marketing and Best Practices recommendations for clients who utilize email marketing. We believe that these recommendations will serve our clients best interests in developing ethical and financially successful email marketing programs.

ABOUT BOCA NETWORKS, INC.

Headquartered in Boca Raton, Florida, Boca Networks is a leading provider of one-to-one email marketing solutions that enable business professionals to create, deliver and analyze direct marketing campaigns and customer communications programs. The company provides a complete email marketing offering, including subscriber acquisition; creative execution; delivery and response management; program data hosting and analytics; bandwidth; collocation; and permission management. Its proprietary email marketing platform enables extensive testing and optimized delivery of richly customized email campaigns using a wide range of content formats, including HTML and rich media.

Boca Networks provides businesses with powerful advantages in the technology marketplace including sophisticated networks (LAN/WAN), hosting, database warehousing, Internet marketing and email broadcast services, database management, Internet service provisioning, e-commerce, co-location facilities, custom workstations and servers, custom cabling (CAT5, 5E, 6 & Fiber), systems integration, network operations center (NOC) build outs, security systems, access control, biometrics, CCTV, and telecom solutions. Our goal is to be your single source

provider for all of your business electronic needs. Boca Networks focus on Productivity to value – delivering better, faster E-Business strategies and solutions that empower our clients to compete successfully in the new economy.

Boca Networks integrates the most advanced end-to-end E-Business solutions quicker and more cost-effectively than any other integrator. This enables Boca Networks' clients to capitalize on the newest solutions, providing them with competitive advantages to increase sales, operational efficiencies and customer satisfaction.

We hope you have found these guidelines valuable, we offer our expertise to insure your online marketing success. Please contact Boca Networks at 561-826-6000 if we can be of any.

CONTACT INFORMATION.

Andrew Paul
Boca Networks.Com, LLC.

561.826.6000 x 110

apaul@bocanetworks.com

www.bocanetworks.com