

## WHITEPAPER

# Email Marketing CAN-SPAM Compliance

## Overview

The CAN-SPAM Act (the “Act”) passed with a nearly unanimous vote in both the House and Senate and was signed into law by President Bush in December of 2003. The Federal Trade Commission (FTC)—along with numerous Internet Service Providers (ISPs)—has since used the law to take action against *bad actors* in the email space.

This whitepaper explores the practical and legal aspects of the CAN-SPAM Act and provides advice about minimizing the risks of email marketing. Email remains one of the most effective vehicles for marketing, communication, and customer retention, and organizations that enact sending best practices will reap the long-term rewards of positive sending reputations, higher customer loyalty, and spotless ISP relationships.

## Email Marketers Beware

The Act is designed to target the most egregious “spammers” and their fraudulent and deceptive practices—not to hinder the sending practices of *legitimate* businesses. However, the CAN-SPAM Act can cause some potential pitfalls for unwary marketers. Those that fail to implement sending best practices and abide by the rules outlined in the CAN-SPAM Act could face fines, costly lawsuits, or—worse yet—prison.

Yet, implementing change across enterprises can be challenging, especially for marketers who don’t realize their organizations are at risk. **It is, therefore, vital that all marketers sending outbound email marketing messages—whether promotional, educational, or otherwise—familiarize themselves with the CAN-SPAM Act and make sure their email marketing programs are compliant.**

## Raising the Bar

The scrutiny of email marketing affects not only legislation and litigation, but also the email processing industry. **With encouragement from anti-SPAM action groups, most ISPs and anti-SPAM filtering technologies have set the bar much higher for marketers than even state and federal laws legally require.** Aimed at reducing the amount of SPAM consumers receive, senders suffering from high rates of undeliverable emails or SPAM complaints are often filtered by ISPs.

**This whitepaper is divided into three sections that will help your organization stay CAN-SPAM compliant:**

- **Part One:** Exploring the CAN-SPAM Act (Page 2)
- **Part Two:** Common CAN-SPAM Pitfalls—And How to Avoid Them (Page 8)
- **Part Three:** Raising the Bar—Permission and Deliverability (Page 13)



## FTC Passes New CAN-SPAM Rules

This whitepaper gives marketers guidance regarding the FTC’s CAN-SPAM Act, including its new rules effective July 7, 2008 regarding:

1. Liability Clarifications (see page 3)
2. Post Office Box Address Notations (see page 5)
3. Unsubscribe Requirements (see page 6)
4. Definition of “Sender” (see page 11)

## How Good is Your Reputation?

Download *The Reputation Equation: Email Marketing & ISP Relationships* from [www.exacttarget.com](http://www.exacttarget.com) to get best practices and tips for improving your ISP sending reputation.



## What is “Criminal?”

The Act prohibits certain “predatory and abusive commercial electronic mail.” Section 4 of the Act generally addresses the manipulation of subject lines, headers, and origination information used to evade detection by ISPs and filters. The section then provides specific penalties for initiators of such acts (and conspirators) including imprisonment, fines, and forfeiture of property used or gained in commission of the offense.

In May 2008, the FTC added a definition of the term “person” in order to clarify that the law’s obligations are not limited to natural persons. This essentially means that the scope of the Act includes individuals, groups, unincorporated associations, corporations, and non-profits. All of these groups must comply with the CAN-SPAM Act.

### Prohibited Under Section 4 of the CAN-SPAM Act:

- **Hiding Email Origin By Using Other Computers (Hacking and Relaying)**  
Accessing a computer without authorization to initiate the transmission of multiple emails is prohibited. Similarly, using a computer to relay or retransmit multiple email messages with the intent to hide the origin of the message is prohibited. Spammers sometimes use different computers—with or without permission—to hide the true origin of an email (thus, evading filters and other blocking techniques used by ISPs).
- **False or Misleading Email Header Information**  
Spammers often try to disguise their “sending” identity by falsifying email “header” information, typically the only portion of the message seen by the receiving mail server. Spammers constantly change and falsify header information in an effort to avoid detection, confuse SPAM filters, and allow them to continue sending SPAM. The CAN-SPAM Act prohibits the initiation of multiple emails with “materially falsified” header information.
- **Deception in Email Registration, Domain Names, and Ownership of IP Addresses**  
The Act prohibits initiating multiple emails from an account where the initiator has registered five or more email accounts—or two or more domain names—using information that materially falsifies the registrant’s true identity. The Act further prohibits initiating multiple emails from an IP address when the initiator has falsely represented he or she is the registrant of the address.

Violations of the above provisions may result in fines or up to five years imprisonment, depending on the seriousness of the violation and other factors. Section 4 of the Act provides for forfeiture of property used in connection with the commission of the offense, gained in, or traceable to the commission of the offense.

**The Act directs the U.S. Sentencing Commission to amend sentencing guidelines to provide specific, appropriate criminal penalties.**

### Beg, Borrow, and Steal

Some spammers try to hide the origin of their emails by using other computers to transmit messages. Such actions are prohibited by the CAN-SPAM Act.

### Civil Actions and Penalties

Section 5 of the Act provides additional protections in the form of civil actions. **However, the law does not provide a civil cause of action for individuals against violators of the CAN-SPAM Act.** Instead, the Act empowers the Attorneys General of each state to pursue violators of certain parts of Section 5 on behalf of the residents of their states.

#### **Additionally, the following guidelines apply to civil actions and penalties:**

- An Attorney General can also pursue money damages, injunctive relief to stop further violations of the Act, or statutory damages up to \$2,000,000.
- Penalty values may be increased for the inclusion of false or misleading information or if circumstances support a finding of aggravated damages.
- Statutory damages can reach up to \$250 per address to which an email is sent.
- A court may increase awarded damages if it finds aggravating circumstances. At its discretion, it may also award attorney fees for successful actions.

Certain federal agencies may file a civil action under the law, and ISPs are provided a civil cause of action against violators of certain sections of the Act. Finally, the Act generally can be enforced by a variety of federal agencies noted in the Act when the actions (or actors) fall within the agency's jurisdiction.

#### Just the Facts Ma'am

The CAN-SPAM Act does not permit suits to be brought by individuals. Only certain federal agencies, state attorneys general, and ISPs can enforce the provisions of the Act.

## Required Commercial Email Content

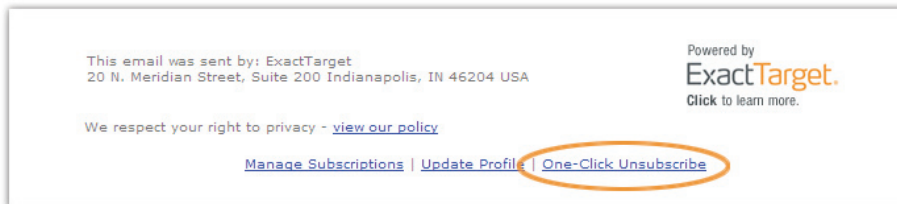
According to the Act, commercial email marketers must include several types of information before sending email messages to any recipient. Marketers should work with their legal counsel to make sure communications are compliant in each content area.

### The CAN-SPAM Act requires the following:

- **All Commercial Email Must Contain a Valid Opt-Out Mechanism**

Every commercial email message must contain a valid mechanism allowing the recipient to unsubscribe (preventing them from receiving any further emails from the associated sender).

Opt-out information must be provided clearly and conspicuously in each message. Companies can provide a generic opt-out from all communications or a more specific menu of options to permit recipients to opt-out of certain types of commercial emails—as long as recipients are also given the option to opt-out of *all* communications.



#### Easy Opt-Out

Every commercial email must include a clear—and ideally instantaneous—opt-out mechanism.

- **Opt-Out Requests Must Be Honored Within 10 Business Days**

The original law allowed the FTC to later set a different “number of days” requirement. However, in May 2008, the FTC reaffirmed its “10 business day” requirement. Most list management tools and Email Service Providers (ESPs) effectively handle unsubscribe or opt-out requests immediately—a best practice all marketers should embrace. However, the ten day window allows for appropriate management of opt-outs in various scenarios, including data synchronization across multiple systems that may only be configured periodically.

- **Sender Must Include a Valid Physical Postal Address**

Senders must include their physical postal address in the body of every email message. In May 2008, the FTC clarified that a post office box or similar postal address will satisfy the requirements of the Act.

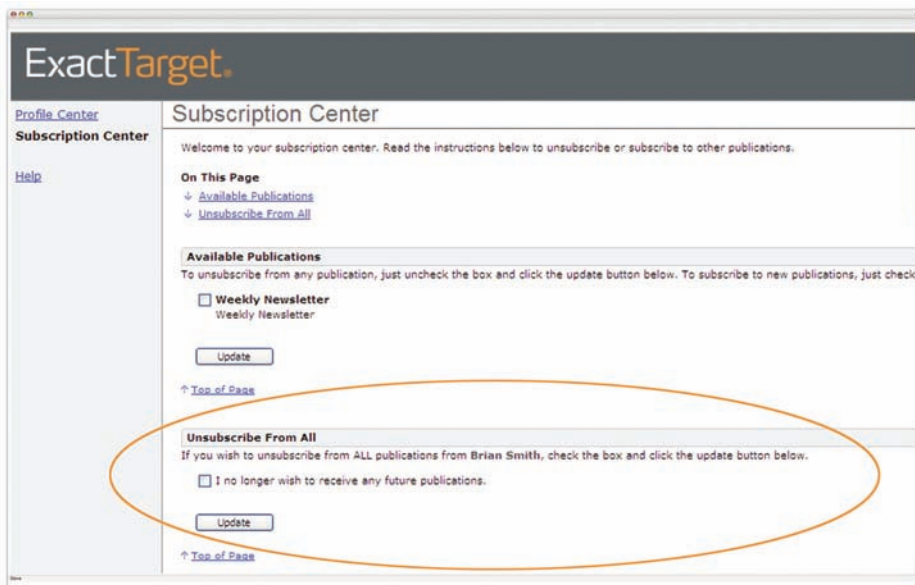
#### What About Post Office Boxes?

As of May 2008, Post Office Boxes (and similar addresses) are acceptable forms of physical address in an email message.

- **Opt-Out Process Must Be Uncomplicated**

In May 2008, the FTC issued updated rules that clarified the opt-out process as required by the Act. The rules indicated the consumer opt-out process may *not* be conditioned on the payment of any fee. In addition, the opt-out mechanism must only rely on the consumer's input of an email address. **The opt-out process cannot require a password (or any other information) which may act as a barrier to the consumer's ability to unsubscribe.**

The opt-out mechanism must rely on either a reply-to mailbox (email-based process) or a visit to a single webpage (web-based process). Assuming a web-based process, any opt-out link in a commercial email message must link directly to a page where the recipient can immediately opt-out of further email messages. **The FTC indicated that multiple steps to verify the identity of the recipient, log-ins, or other account confirmations are unnecessarily burdensome and no longer allowed.**



#### Subscription and Profile Centers

Subscription Centers should include clear opt-out links (without requesting any more subscriber information than an email address). ExactTarget automatically adds an “Unsubscribe From All” link to your Profile Center to follow this best practice.

- **If Unsolicited, An Email Must Provide a Clear Notice That It Is An Advertisement**

The law does not make a recommendation for the specific language to be used to fulfill this requirement, or how it is to be positioned in the email. Note: this does not make unsolicited commercial emails acceptable to ISPs; they can—and—do set higher “permission-based” standards for email marketers.

- **Operative Opt-Out Mechanism Requirement**

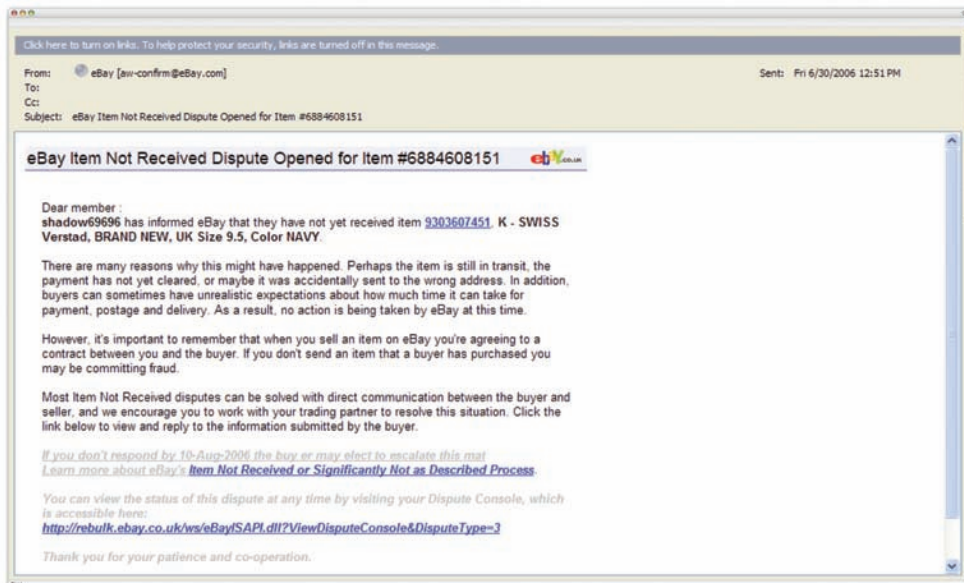
A valid return address (or comparable Internet-based communication technology) must allow a recipient to opt-out of future email communications, and the operative opt-out mechanism must be available for at least 30 days following a mailing. The Act provides leniency for temporary outages.

- **Senders Must Label Sexually-Oriented Messages**

For emails containing adult or sexual content, senders are required to include the warning, “SEXUALLY-EXPLICIT.” in the subject line. The Act outlines additional requirements and penalties for messages involving sexually-oriented material.

- **No False, Deceptive, or Misleading Email Transmission Information or Subjects**

This requirement focuses on deceptive practices often used by spammers to avoid filters and encourage recipients to open a message and respond to a false offer or scam. Note: The Act specifies that emails containing accurate identification of the message’s initiator are not classified as false or misleading.



### Mistaken Identity

Sample “phishing” email illustrates sender posing as a recognized brand in order to trick recipients into sharing personal information.

## Part Two: Common CAN-SPAM Pitfalls—And How to Avoid Them

At first glance, the CAN-SPAM Act establishes fairly basic rules for an organization to follow. However, given that this law is constantly evolving (as seen when the FTC enacted four new rules in May 2008), new details and judicial interpretations will surely follow. Email marketers must remain alert to changes and proactively avoid the common pitfalls outlined below.

### 1. Develop and Enforce an Enterprise-Wide Unsubscribe or Opt-Out Process

The Act's opt-out requirement states: "Require such email senders to give recipients an opportunity to decline to receive future commercial email from them and to honor such requests."

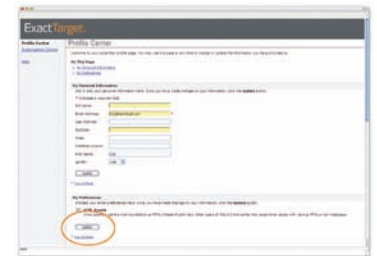
To ensure your organization is compliant, ask yourself these important questions:

- Is your company technically prepared to manage and maintain not just one—but potentially several—"suppression" lists of email recipients who don't want to receive commercial email?
- Do you have a method to control opt-out requests and suppression lists across all departments within the enterprise?
- Do you have the technological capability and capacity to log and maintain a master suppression list and several more specific suppression lists simultaneously?
- Do you have the decision-making and communication procedures in place to determine when a subscriber has opted-out of *all* (versus only some) future communications, and to inform your database administrator of subscriber changes?
- Can your company make appropriate permission changes within ten business days of that opt-out request as required by the Act?
- Can database updates be communicated to all locations of your company's enterprise that use this data quickly enough to prevent another area of the company from contacting an unsubscribed user after 10 days have passed?

Addressing these questions can be challenging, especially for organizations with disparate data sources, decentralized marketing programs, several physical locations, or multiple divisions or processes. But the stakes for ignoring the Act's requirements are high, and a failure to properly handle opt-out requests can lead to prosecution and severe penalties.

**Organizations must make a concerted effort to not only implement the proper technology to handle opt-out processes, but also to ensure the philosophy of honoring that opt-out is adopted at every single customer touch point—from the CEO to a local sales representative.**

If systems cannot support centralized unsubscribe list management efforts, organizations should consider offering employee education and training about the risks associated with commercial email marketing and the CAN-SPAM Act.



#### Get Organized

Every ExactTarget email automatically provides a link to a Profile Center, which gives subscribers the option to opt-out of specific communications—or all communications. What does that mean for the marketer? Organized suppression lists—and *peace of mind*.

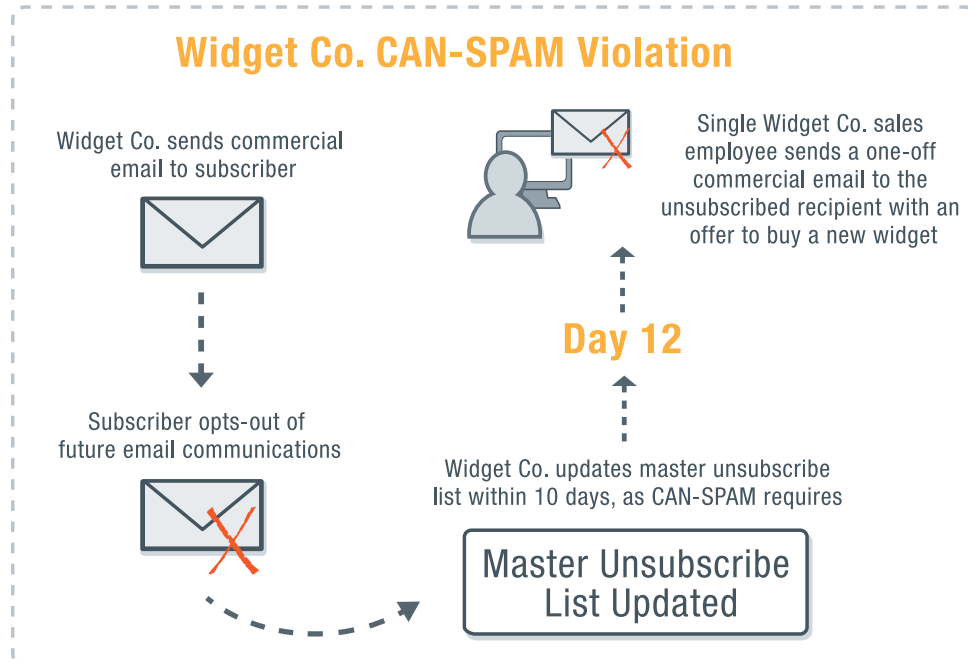
**One option for managing email unsubscribes in a central location is engaging a single email provider.** ESPs like ExactTarget have the ability to manage unsubscribe data in a centralized and secure location, instead of managing data across multiple divisions of the organization.

In addition to the fact that ESPs have experience managing email and the complexities of email list removal, data centralization provides an easy way for marketers to streamline multiple email communications and clean subscriber data. It also provides enterprise-level security that email assets are stored in a secure, encrypted environment.

## 2. Enforce CAN-SPAM Compliance with Every Email and Every Employee

Individual employee emails present a substantial risk to companies lacking a central control point over their email communications. As the Act provides, organizations and their agents (employees, contractors, etc.) must “honor the recipient’s request” to stop further mailings.

**Legal ramifications can result from as few as one employee’s poor decision to send an email to a recipient who has opted-out.**



### The Email Delivery Guru

Look for more insights about the world of CAN-SPAM compliance and email marketing deliverability from ExactTarget’s Director of Privacy & Deliverability.

Check out Al Iverson’s blog, *The Email Delivery Guru*, at [www.exacttarget.com](http://www.exacttarget.com).

### It Only Takes One

Be sure every employee understands proper permission procedure, and that every commercial email is compliant with CAN-SPAM. One mismanaged commercial email is enough to cause serious trouble with the FTC.

### 3. Develop a Strategy for Capturing Affirmative Consent

CAN-SPAM provides advantages to organizations that only send to recipients who have opted-in to their email communications. Per the Act, affirmative consent (also referred to as permission marketing, explicit opt-in, or direct consent) exists if a recipient has “expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient’s own initiative.” **When affirmative consent is obtained, commercial labeling requirements no longer apply.**

For example, a company that promotes products through an email promotion to consumers who have willingly provided their email addresses to receive such promotions does not need to include an “advertisement” label on their emails. This is advantageous as such advertising labels which can be easy targets for SPAM filters.

### 4. Don’t Send Unsolicited Email Messages

The law states that in the case of unsolicited commercial email messaging, all messages must be clearly identified as an advertisement or solicitation (though the Act does not specify the exact labeling method required). Email marketers need to be aware that ISPs commonly block email messages with such labels. So senders who have to label a message as a solicitation or advertisement will nearly guarantee that it will be widely filtered or blocked by ISPs.

**While the law effectively allows the sending of unsolicited commercial email if all applicable requirements are followed, it does not prohibit ISPs and SPAM filtering service providers from discarding or refusing to deliver unsolicited mail.** The vast majority of ISPs and ESPs have policies prohibiting the sending of unsolicited commercial email messages from their networks (or to their users) and are quick to block messages they deem unsolicited commercial email. **As a best practice, companies should never send unsolicited email messages.**

#### Walks Like SPAM, Talks Like SPAM

The law allows the sending of unsolicited commercial email if applicable requirements are followed, but ISPs and SPAM filtering service providers are still allowed to discard or refuse to deliver unsolicited email.

**The law might also cause an organization to ask what should happen when a consumer visits its website and provides an email address as part of a request for information.**

Does the Act require them to send email in response to the inquiry which includes an opt-out, valid physical address, and reply address?

**The Act defines a commercial electronic mail message as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service....”** Therefore, if an email is a first communication with a recipient and is truly in response to the consumer’s inquiry, arguably the primary purpose is not to advertise or promote. Rather, its purpose is to respond to an inquiry from the consumer. However, subsequent email communications or promotions for products and services should include an opt-out, valid physical address, and reply address per the Act.

**Creating a method to capture affirmative consent—such as an opt-in checkbox on a web form—provides clarity about whether future subscriber emails are warranted.**

Though a physical postal address and unsubscribe mechanism are required, a company might be able to avoid the commercial labeling requirement if it secures affirmative consent. For more information on affirmative consent and permission email marketing, see Part Three of this whitepaper.

## 5. Be Careful When Email Relates to a Particular Business Segment

The Act provides, “if an entity operates through separate lines of business or divisions and holds itself out to the recipient throughout the message as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of business or the division shall be treated as the sender of such message for purposes of this Act.”

Under the law, a “sender” is defined as the entity whose goods or services are advertised in a commercial email message. Updated rules provide a clearer definition of “sender,” and make it easier to determine which of multiple parties advertising in a single email message is responsible for complying with the Act’s opt-out requirements. **The sole sender appearing in the from line of the email becomes the designated sender of the message and must comply with all provisions of the Act (such as listing a physical postal address and providing an opt-out mechanism).**

In other words, if a particular business division sends an email which indicates it is an advertisement from that division, the parent organization can continue to send emails to recipients that have opted-out to email communications from the division.

Organizations should implement procedures and educate their divisions, business units, and other affiliates to clearly indicate the email sender on every message—and specifically to identify the business division from which the subscriber can opt-out. If a commercial email transmission could be mistakenly understood as originating from the parent organization, it is even more important to clearly identify the particular line of business or division as the sender. **The most conservative approach is to eliminate the recipient from all of the lists of the related companies.**

### When In Doubt, Opt Them Out

If subscribers might assume their opt-out applies to more than one business unit, remove them from all related lists—just to be on the safe side.

## 6. Avoid Misleading Email Subject Lines

In the past, marketers could achieve significantly higher response rates by using promotional language and “teasers” in a subject line that enticed recipients to open the email.

For example, a legitimate anti-virus software company might use the subject line: “Your computer may be infected” to encourage recipients to open its message. But today, the same subject lines are easy targets for email SPAM filters and may actually violate the Act.

Companies need to educate employees and develop internal communication processes to ensure that its marketers are aware of similar constraints on their creative licenses. Specifically, companies should develop a review process to ensure subject line restrictions are upheld. **And when in doubt, marketers should consider the standpoint of “the reasonable recipient” to determine if a subject line is misleading or could be misinterpreted.**

## 7. Obtain Opt-In for Wireless Communications

The CAN-SPAM Act requires that companies obtain opt-in for commercial email messages sent to wireless devices or cell phones. Under FCC 04-194, any commercial email sent to a wireless device domains must obtain express prior authorization and an e-signature for all wireless domain subscribers.

**While some domains in this category are excluded, a full list of affected domains can be found here: <http://www.fcc.gov/cgb/policy/DomainNameDownload.html>.**

The net effect of these restrictions and requirements is such that sending commercial email messages to addresses at “mobile service” domains is not allowed. ExactTarget keeps a synchronized copy of all of the “mobile service” domains identified by the FCC (based on information provided by those service providers) and prohibits users from importing addresses that are prohibited and would violate the CAN-SPAM Act.

## 8. Refrain from Harvesting Email Addresses & Dictionary Attacks

Email Harvesting typically refers to the automated harvesting of addresses from websites. Spammers often employ this tactic using software developed specifically for the purpose of harvesting email addresses.

Dictionary Attacks refer to spammers’ tactic of guessing addresses using an algorithm or dictionary-type tool to search for email addresses. Dictionary Attacks can produce email strings like ajohnson@hotmail.com, bjohnson@hotmail.com, cjohnson@hotmail.com, etc.

The CAN-SPAM Act generally provides for damages of \$250 per violation up to \$2 million dollars (or more for violations involving a false or misleading transmission of information), but these damages may be increased for willful violations or violations where Email Harvesting or Dictionary Attack tactics are used. For civil action suits initiated by ISPs, damage caps for these violations are somewhat reduced.

### Times are Changing

And your subject lines must change with them. The “teaser” phrases that were successful in the past often throw red flags for today’s SPAM filters.



### Email Marketing for the Third Screen

For more trends and tips regarding mobile email marketing, download the *Email Marketing for the Third Screen* Whitepaper from [www.exacttarget.com](http://www.exacttarget.com).

### Part 3: Raising the Bar—Permission and Deliverability

Some CAN-SPAM Act opponents do not believe that the Act effectively reduces SPAM. They argue that by allowing unsolicited commercial email as long as an opt-out and physical addresses are present, the government is essentially legalizing SPAM.

However, the anti-SPAM community and ISPs have long opposed any email marketing situation where affirmative consent does not exist. ISPs filter billions of SPAM messages daily, and **SPAM prevention is seen as a worthy cause for millions of subscribers whose inboxes are frequently flooded with fraudulent emails, bogus health claims, and pornography.**

CAN-SPAM is somewhat sympathetic to the plight of ISPs and states that it shall have “no effect on policies of Internet access service.” The Act, therefore, does not preempt the more stringent SPAM requirements of ISPs (unlike the laws of certain states which are preempted by the law).

**To improve deliverability with ISPs, email filtering companies, and anti-SPAM blacklist organizations, senders should consider the following recommendations.**

#### 1. Play by the Rules of ISPs and Filtering Companies

Inboxes are more crowded than ever, and many ISPs are diligent about blocking all messages they believe may be SPAM. However, an unfortunate portion of these blocked emails originate from legitimate companies that are simply unaware of underlying ISP SPAM filtering logic. **As a result, legitimate emails are often filtered (a scenario known as “false positive filtering”) before ever reaching their intended recipients.**

ISPs often combine content filtering mechanisms—which scan email subject lines and body content to determine which emails are SPAM—with other types of filters that check for number of complaints received for a specific sender. They may also look at the number of undeliverable emails generated by a specific mailing when deciding whether to filter a message. **Senders who deploy high quantities of email promotions, send to dirty lists, or generate many complaints (who “look like spammers” to ISPs) are blocked.**

Though ISP filters are built on averages (and are therefore imperfect), they are a reality of sending commercial email in today’s SPAM-sensitive environment. False positive filtering sometimes occurs for emails from legitimate marketers due to the commercial content of the messages. However, false positives are most prevalent with email that is “unwanted” by recipients. **Organizations should not underestimate the power of ISPs and other organizations using SPAM filtering—their control over the delivery of email messages only continues to increase.**



#### Deliverability Report Card™

ExactTarget’s Deliverability Report Cards™ help marketers keep track of their standing with major ISPs, SPAMCop complaints, and other essential delivery metrics.



#### Are You Getting Through?

Monitor your delivery success with major ISPs with eDelivery Tracker, one of several advanced deliverability tools available with ExactTarget’s Inbox Detective™.

## 2. Reduce SPAM Blocking with Permission-Based Email Marketing

Permission-based email marketing is extremely important to the success of any company’s email marketing efforts, and provides significant deliverability and economic benefits. Also known as “opt-in email marketing,” permission-based email marketing describes sending email to *only* those recipients who have asked to receive information from a specific company via email. Organizations should strive to use standards set forth by eMarketing pioneer Seth Godin, author of *Permission Marketing*, who proposes all marketing messages must be “anticipated, personal, and relevant.” **By opting-in to email communications, a subscriber has given permission to receive a type of message—and it is the sender’s responsibility to deliver (not abuse) that relationship.**

### Building a Permission-Based Opt-In List

Developing a permission-based email list takes time, but the benefits far outweigh the effort. **An organization focused on list growth can effectively build its permission-based email lists by capturing opt-ins at each customer/prospect touch point—like at point-of-sale, on a sign-up form, kiosk, website, or during a phone call.** As long as the subscriber willingly requests information via email, his or her opt-in can be considered permission-based.

Giving subscribers the power to choose their communication types, channels, and frequencies, helps companies build higher quality permission lists. Subscribers who specifically request information via email are less likely to file SPAM complaints, and their messages are less likely to be filtered to the junk folder or discarded. **Mailing to email addresses gathered without subscriber knowledge or approval violates the Act. Such activities will generate more SPAM complaints that damage the sender’s reputation with ISPs and jeopardizes future deliverability success.**

Enterprises must also be wary of the ways in which their *employees* gather email addresses. As opposed to Email Harvesting and Dictionary Attacks, there are several ways in which an employee might unwittingly gather email addresses in an unsolicited fashion.

For example, imagine Joe is an employee of XYZ Company. While attending a networking function, he collects business cards from several prospective clients. Although Joe has not asked each of these prospects permission to send them email communications, he returns to work the following day and adds them to his company’s master subscriber list. Mailing to these individuals violates the CAN-SPAM Act, and could lead to ISPs blocks, SPAM complaints, blacklists, or civil actions against XYZ Company.

The best practices in this situation would have been for Joe to instead follow up with the prospective clients with a phone call. During the call, he could gain each person’s consent and add his/her name to XYZ’s mailing list. Alternatively, he could focus on capturing written consent at the networking function before adding the email addresses to the list. Or, Joe could send a personal email to each prospective client to express his pleasure in meeting the prospect and to request permission to send information in a future communication.



**Permission-Based Email Marketing**  
 Want to learn how to execute an effective permission-based email marketing program? Download ExactTarget’s *Permission-Based Email Marketing Whitepaper* at [www.exacttarget.com](http://www.exacttarget.com).



**List Growth the Right Way**  
 Learn how to build a permission audience-based list the right way by downloading the *Hershey Entertainment & Resorts Case Study* at [www.exacttarget.com](http://www.exacttarget.com).

### 3. Move to Double Opt-in to Reduce Threat of Blacklisting

Third-party anti-SPAM blacklists (also called “block lists”) are SPAM-filtering plugins (often free) that the majority of email server administrators can subscribe to. **Senders who violate perceived best practice guidelines often find their sending IP addresses listed on one or more of these blacklists.** Email servers that subscribe to the blacklist are then likely to reject all email sent from blacklisted sender IP addresses. This can have a substantial impact on email deliverability as a substantial percentage of an organization’s email is filtered before reaching the inbox.

Organizations that find their IP addresses on a blacklist are often required to prove they use permission-marketing practices before they will be removed from the blacklist. Blacklist removal requirements can vary greatly, and some blacklists may require that an ISP or ESP terminate services to the organization that “caused” the blacklisting before the IP address will be removed.

To avoid blacklisting, organizations should always follow opt-in best practices. **Permission may be qualified into two categories: single and double opt-in.** Single opt-in is simply capturing approval from a subscriber to send them email. Double opt-in (also called confirmed opt-in) utilizes email address verification to ensure permission and log opt-in consent from the end recipient.

**In a double opt-in scenario, a welcome message (called an “opt-in confirmation”) email is sent to the subscriber.** The recipient is considered opt-in *only* if he or she clicks on the link contained in the opt-in confirmation message. If the end recipient does not click, he or she should not to be considered opt-in or not receive any further messages.

Your organization may want to consider using double opt-in to:

- Keep Your Lists Clean**  
 By requiring a second opt-in confirmation, organizations reduce the risk of adding misspelled or fraudulent email addresses to their list. Mailing to bogus addresses raises the number of undeliverable emails and increases the likelihood of filtering. It can also result in mailing to “SPAMtrap” addresses put in place by ISPs and email filtering companies to trap unwary companies.
- Be Above Reproach**  
 Double opt-in email addresses provide assurance—as well as an electronic record—that affirmative consent is in place should the company need to validate sending practices or defend against potential litigation.
- Guard Against SPAM Complaints**  
 Double opt-in subscribers are much less likely to complain or misidentify an email as SPAM. Maintaining a low complaint rate is key to preventing ISP blocking and filtering.

#### Spread the Word

One email blocked from one employee’s email address can put the entire enterprise at risk for email filtering and blocks.



#### Perfect Your Opt-In Process

Request a copy of the *Opt-In Best Practices Data Sheet* from an ExactTarget representative, and make sure your processes are above reproach.

#### 4. Maximize Delivery with Opt-in Reminders

Since subscriber complaints are a large component of the logic used by many filtering mechanisms, subscriber recognition of an organization and a recollection of their opt-in determines the likelihood that a recipient will file a SPAM complaint. **Subscribers receiving email that is expected, branded, and easy to recognize are unlikely to mistake a message as SPAM—which in turn reduces the potential for filtering.**

For example, the best practice to improve recognition at the time of website name capture is for an organization to list the type of email which will be sent, the name of the publication, its frequency, and who it will be “from.” This sets expectations with subscribers and reduces the chance of complaints and filtering.

Another step many organizations are taking to improve recognition and add credibility to their mailings is adding a short text reminder at the top of each email. For example: *“You are receiving this mailing because you opted-in to receiving emails from xyzco.com. Please add abc@xyzco.com as a Safe Sender in your address book.”*

Providing text that asks each subscriber to add the sender to his or her address book will help organizations make it to the inbox, rather than having their messages routed to the “bulk” or “junk” folders. Major ISPs—such as AOL®, Yahoo!®, MSN®/Hotmail®, and Microsoft® Outlook®—route email sent from senders on their users’ safe sender lists past SPAM filters.

#### 5. Maintain a Consistent From Address and Subject Line Recognition

It is important for organizations to maintain a consistent “from name” in their emails for a number of reasons. First, it is an important element of recognition, and studies prove that a majority of email users first look at the “from name” when determining whether or not they open a message. **Organizations that use a consistent “from name” also benefit because their subscribers grow accustomed to receiving emails from a particular address and begin to anticipate these messages.** Second, maintaining a consistent from name will help organizations leverage the benefits of being in their subscribers’ safe sender address books.

**Another step organizations can take to ensure their subscribers recognize their emails is to include the name of their organization in the email subject line.** The CAN-SPAM Act requires the subject line of a commercial email not be misleading or fraudulent. But going a step farther by adding the company name to the subject line not only adds credibility, but also increases recognition and reduces the potential for subscriber complaints and subsequent filtering.

#### Summary

With the passage of the Federal CAN-SPAM Act, marketers need to be aware of both the practical and legal aspects of sending commercial email. The requirements of the Act will have significant impact on unwary organizations or those that fail to adjust internal procedures appropriately. However, organizations that take the proper steps to overcome challenges and risks will reap the rewards of subscriber loyalty in the long run.

#### Consult Your Legal Counsel

These materials do not constitute specific legal advice and may not address all aspects of a legal development relevant to your circumstances. Consult legal counsel to determine how laws apply to your specific situations. Further, these materials are not intended to create, and receipt of them does not constitute, a lawyer-client relationship.

*Copyright ExactTarget and Ice Miller 2008*