Customer Paradigm
Customer-Centric Thinking

4204 Greenbriar Blvd
Boulder, Colorado 80305
303.473.4400 x 22
www.CustomerParadigm.com

Understanding the CAN-SPAM ACT of 2003

Q: We don't send unsolicited email. Why do I need to read this?

A: Even if your company or organization only sends permission-based email, the CAN-SPAM Act may require you to change how you send your permission-based email in order to understand the new legislation. For example, you may be required to include your postal address in all outbound email messages (see below for more details).

IMPORTANT DISCLAIMER:

THIS SUMMARY IS PROVIDED FOR GENERAL INFORMATION ONLY, AND SHOULD NOT BE USED IN PLACE OF QUALIFIED LEGAL COUNSEL. THE COMPLETE TEXT OF THE CAN-SPAM ACT IS INCLUDED AT THE END OF THIS DOCUMENT. CUSTOMER PARADIGM IS NOT RESPONSIBLE FOR ERRORS OR OMMISIONS. USE THIS SUMMARY AT YOUR OWN RISK.

Permission Email Policy:

Customer Paradigm recommends opt-in, permission-based email marketing and messaging. Sending unsolicited commercial email (UCE) will likely result in consumer backlash, damage to your reputation, brand, and blacklisting by anti-spam organizations of your domain (which will prevent you and anyone else on your domain from sending email to much of the Internet).

The fact that so many people – 136 million active email users in the US alone – put up with porn, body-part extension offers, herbal extracts, the chance to earn $15,000 a week from the comfort of their home – attests to how important email is in the lives of the everyday citizen.

Bottom line: Don't send unsolicited email. This guide is meant to help legitimate businesses and organizations understand the new CAN-SPAM Act of 2003.

Background:

When the "Do Not Call" registry website was launched during the summer of 2003, it was an instant hit with millions of people. No longer would anyone who signed up have to suffer through unwanted telemarketing calls during dinner. Lawmakers in Congress quickly realized that passing such common-sense legislation that affects the everyday lives of citizens would be an asset during the next election.

Spam, or Unsolicited Commercial Email (UCE), remains another significant intrusion into the lives of ordinary Americans. According to some estimates, UCE makes up more than 50% of all email. UCE is expected to cost U.S. businesses more than $10 billion problem in 2003.

Approximately 45% of the U.S. population has an email account, according to a U.S. Department of Commerce study in September 2001 (the latest data available). Eighty-four percent of email users check their email account frequently. In the past ten years, email has grown from tech

4204 Greenbriar Blvd
Boulder, Colorado 80305
303.473.4400 x 22
www.CustomerParadigm.com

obscurity to one of the dominant ways that people communicate. From grandparents seeing photos of their grandchildren via email, to businesses sending documents and information effortlessly, people rely on email to keep them connected.

Thirty-five states have passed conflicting and contradictory state laws to deal with the rise in UCE, but until recently Congress had done little to address the issue of UCE. California's restrictive anti-spam law was set to take effect on January 1, 2004, but is pre-empted by the federal "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (also known as the CAN-SPAM Act, which takes effect January 1, 2004). While critics claim the legislation will due little to halt unsolicited email (especially UCE that is sent from overseas), the legislation is a win for businesses and organizations that have had difficulty complying with a confusing patchwork state laws.

Summary of CAN-SPAM Act of 2003:

Under the CAN-SPAM Act of 2003, your email messages will likely fall under one of the two categories:

1. Relationship / Transactional Messages:

- Messages sent to complete a transaction or sale or deliver goods / services
- Warranty, product updates, upgrades, or recall information
- Safety or security information about a product used or purchased by recipient
- Change in terms or features of a subscription or service
- Account balance information

→ If #1, then you must not use fraudulent headers:

- **Must Not Use Fraudulent Headers:**
  - You can't create an email account or a domain with false information in order to send non-traceable messages.
    - You must use accurate information
  - You can't disguise the origin of the message
  - The FROM: line can't be deceptive or misleading
  - The Subject line can't be deceptive or misleading
  - You can't promote a business or allow your business or organization to be promoted by using false information in the headers of emails.
  - **Recommendations:**
    - Make sure that your domain name is registered with the correct and current information, including postal address, a working email address and phone number.

2. Commercial Electronic Messages:

- Primary purpose is to promote a product, service, or content on a Website operated for commercial purpose
- *Most marketing-related email messages will likely fall into this category*

→ If #2, then you must comply with the following requirements:

4204 Greenbriar Blvd
Boulder, Colorado 80305
303.473.4400 x 22
www.CustomerParadigm.com

- **Opt-out / Unsubscribe Mechanism:**
  - Recipient must be able to reply to message to unsubscribe or remove themselves from your list
  - Or, you can provide a link to an unsubscribe page, where the user can select which newsletters and types of emails he or she wants to receive from you.
  - You must remove unsubscribe requests within 10 days
  - **Recommendations:**
    - Send Confirmation email to recipient, informing them that they have been removed from list
    - Use both 'reply-to' unsubscribe method and link method for handling unsubscribe requests
    - One common source of frustration in the unsubscribe process is that people often sign up to a list with one email address, but then try to unsubscribe from the list with another. If you are able to mail-merge the user's email address into the bottom of the message (this often requires special software), you may be able to avoid this issue.

- **You must have a "valid physical postal address of the sender" in all commercial email messages.**
  - **Recommendations:**
    - This is perhaps the requirement that will be the easiest to forget, as electronic communication tends not to use postal information.
    - Also consider including a telephone number in each message that you send out.
    - If you're trying to decide between using a PO Box or your physical address, the act stipulates a "valid physical postal address of the sender" – err on the side of caution and use the physical address that is able to receive postal mail.

- **Functioning Return Email Address:**
  - Must remain active for at least 30 days after the message was sent.
  - The CAN-SPAM Act allows for unexpected or temporary technical problems, if this was beyond the control of the sender. Problems must be corrected within a reasonable period of time.

  - **Recommendations:**
    - Make sure that the email account's mailbox doesn't fill up. Most email accounts have size limits for storage space (often 2-5 megabytes).
      This is something that is usually within the control of the sender
    - A formula for determining how much space you might need:
      - Required Size of Mailbox = (Size of messages in KB) x (Number of messages sent) x (bounce %)
      - Thus if you send a 10 kb message to 10,000 people and have 30% of the messages bounce-back or have a vacation or out-of-the-office autoresponder, you will need at least 30 megabytes of storage for the account.

- **ADV warning label in subject line**
  - Only required if you don't have express permission to send an email to the recipient
  - "Affirmative Consent" is defined as…
    - Recipient has expressly consented to receive the message
  - ADV or other label will be determined by FTC at a later date
  - **Recommendations:**

4204 Greenbriar Blvd
Boulder, Colorado 80305
303.473.4400 x 22
www.CustomerParadigm.com

- When asking for "affirmative consent" from the recipient, use either:
  - A confirmed opt-in:
    - Recipient receives a notification email confirming their request to receive an email
  - Double Opt-in:
    - Recipient receives a notification email
    - Recipient is not added to list unless they click on a link in the email or reply to the notification message
    - This method confirms control of the email account

- **Must have Valid Header Information / Not Use Fraudulent Headers:**
  - You can't create an email account or a domain with false information in order to send non-traceable messages.
    - You must use accurate information when registering a domain or an email address.
  - You can't disguise the origin of the message
  - The FROM: line can't be deceptive or misleading
  - The Subject line can't be deceptive or misleading
  - You can't promote a business or allow your business or organization to be promoted by using false information in the headers of emails.
  - **Recommendations:**
    - Make sure that your domain name is registered with the correct and current information, including postal address, a working email address and phone number.
    - Make sure that abuse@ and privacy@ email addresses are working for your domain, and that someone is in charge of responding to messages.

- **You mail server must not have an open relay / allow others to send email through your servers without your permission.**
  - **Recommendations:**
    - Make sure that your IT department checks your computers for open mail relays.
    - Make sure that only valid, authorized people are able to send email messages through your computers or servers:
      - POP before SMTP Authentication: User must check their POP email account with a username/password before they are able to send messages.
      - Username / Password for Sending: User must login to the SMTP or outbound email server with a username and password before they are able to send messages.

- **You must not use an open relay or send via a computer with a username / password where you don't have permission.**
  - **Recommendations:**
    - Don't send your messages through someone else's server without their express permission.

- **List Management:**
  - Don't use lists that were built using dictionary attacks, harvested emails, or randomly generated email addresses.

4204 Greenbriar Blvd
Boulder, Colorado 80305
303.473.4400 x 22
www.CustomerParadigm.com

  - If you collected email addresses on a website with a posted privacy policy (and the privacy policy stated that you wouldn't give, sell or transfer their email address), then you can't give, sell or transfer their email address.
  - If you are selling a list of email addresses, you must not include anyone who asked to be removed from the list.
  - **Recommendations:**
    - If you said you were not going to do sell people's email addresses, then don't sell their email addresses.
    - The FTC has enforced similar privacy violations in the past with substantial fines.
    - Get qualified legal counsel. This gets very complicated very quickly.

- **If you have Sexual Content:**
  - If you don't have "affirmative consent" from the recipient that they want to receive your email messages (see above), you must use a warning label that labels the content as sexual in nature.
  - The warning label has not yet been determined, but will be decided by the FTC within 120 days of January 1, 2004.
  - 5 year jail penalty for non-compliance.
  - **Recommendations:**
    - **Get qualified legal counsel.**
    - **Use a double-opt-in method for building your permission-based list.**

"Do Not Email Registry":

- Within six months, the FTC must issue guidelines and a report that explains the practical, technical, security, privacy, enforceability or other concerns that the FTC has about the registry, as well as how the registry would be applied with respect to children with email accounts.
- The FTC can't implement a Do Not Email Registry before September 2004.

Also Authorized:

- **Study for the effectiveness of the CAN-SPAM Act**
  - Report due within 24 months
- **System to reward people who turn in violators of the CAN-SPAM Act**
  - Reward will be at least 20% of the fine
  - No system is specified; report from FTC due within 9 months.
- **Wireless Commercial Message Rules:**
  - Help protect consumers from unwanted mobile service commercial messages
  - Report due within 270 days.

Enforcement:

- **FTC can enforce the CAN-SPAM Act with the following:**
  - 5 years in jail for repeat offenders who also commit a felony
  - 3 years in jail for first time offenders

Customer Paradigm
Customer-Centric Thinking

4204 Greenbriar Blvd
Boulder, Colorado 80305
303.473.4400 x 22
www.CustomerParadigm.com

  - Confiscation of proceeds from mailing as well as any computers, software, technology or equipment used during the offense.
- **State Attorney's General can enforce the CAN-SPAM Act with a civil action:**
  - $250 / message, up to $2 million
  - If fraudulent information used in headers, no upper limit
- **ISPs can enforce the CAN-SPAM Act with a civil action:**
  - Damages of actual monetary loss
  - Or, $25 / email, up to $1 million. If fraudulent information is used in the headers, damages of $100 / email with no upper limit.

Email Deployment Checklist:

- ❑ **Valid FROM email address?**
- ❑ **SUBJECT line not misleading?**
- ❑ **Email address is working and available for at least 30 days?**
- ❑ **Size of email address is sufficient to hold bounced / returned messages?**
- ❑ **Physical Postal Address included in message?**
- ❑ **Domain name registration information accurate?**
- ❑ **Opt-out / remove system working properly?**
- ❑ **Warning label in subject line if non-affirmative consent?**
- ❑ **Your mail server is not an open relay or gives non-authorized users access?**
- ❑ **You have permission to send via the appropriate mail server?**
- ❑ **List was gathered appropriately (see above)?**
- ❑ **Spellcheck message (to prevent typooos and misssteakes)?**
- ❑ **Common Sense Test: Does the message make sense to a potential recipient?**
- ❑ **Message is relevant to target audience? Somehow adds value to their lives?**
- ❑ **Personalization is used properly?**
- ❑ **Test messages to make sure they render properly in different email platforms?**
- ❑ **Privacy Policy posted on Website?**
- ❑ **Abuse@ & privacy@ email addresses working?**
- ❑ **Are messages flagged by anti-spam filters?**
- ❑ **Is your server Blacklisted?**
- ❑ **Is your server Whitelisted?**
- ❑ **Names are not all pasted into TO: line?**
  (Note: this mistake cost Eli Lilly $160,000)

Questions? Need to help with understanding CAN-SPAM?
Call: 303.473.4400 x 22 today.